Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools

Koops, E.J.; Bodea, G.; Broenink, G.; Cuijpers, C.M.K.C.; Kool, L.; Prins, J.E.J.; Schellekens, M.H.M.

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

UNIVERSITEIT VAN TILBURG

TNO innovation for life

Juridische scan openbrononderzoek

Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools

Bert-Jaap Koops
Gabriela Bodea
Gerben Broenink
Colette Cuijpers
Linda Kool
Corien Prins
Maurice Schellekens

Tilburg University
TILT – Centrum voor Recht, Technologie en Samenleving
Postbus 90153
5000 LE Tilburg
<e.j.koops@uvt.nl>

TNO
<gabriela.bodea@tno.nl>

juli 2012

Inhoudsopgave

Afkortingen 4
Managementsamenvatting 5

1. Inleiding 7
   1.1. Achtergrond: systemen voor openbrononderzoek door autoriteiten 7
   1.2. Doelstelling en vraagstelling 8
   1.3. Afbakening 8
   1.4. Methoden van onderzoek 9
   1.5. Leeswijzer 9

Deel I. Juridische aspecten

2. Privacy en bescherming van persoonsgegevens 11
   2.1. Inleiding 11
   2.2. Privacy: art. 10 Gw en art. 8 EVRM 12
      2.2.1. Privacy en gegevensbescherming 12
      2.2.2. Het recht op privacy, Handvest en EVRM 13
   2.3. Wet bescherming persoonsgegevens 14
      2.3.1. Toepasselijkheid Wbp 14
      2.3.2. De begrippen 'verantwoordelijke' en 'bewerker' 16
      2.3.3. Een gelaagd systeem van gegevensbescherming 17
      2.3.4. Privacyaspecten van het loggen van iRN/iColumbo-gebruik 24
   2.4. Internationale aspecten 25
   2.5. Korte blik op de toekomst 26
   2.6. Conclusie 26
3. Auteursrecht en databankenrecht 28
   3.1. Inleiding 28
   3.2. Auteurswet 28
      3.2.1. Wat is beschermd? 28
      3.2.2. Ruimte voor omgang met werken 29
      3.2.3. Auteursrechten op tools 31
   3.3. Databankenwet 32
      3.3.1. Wat is beschermd? 32
      3.3.2. Ruimte voor omgang met databanken 32
   3.4. Internationale aspecten 33
   3.5. Korte blik op de toekomst 34
   3.6. Conclusie 35
4. Wetgeving met betrekking tot eindgebruikers 37
   4.1. Politie 37
      4.1.1. Grondslag voor bevoegdheden 37
      4.1.2. Eisen aan gebruik van bevoegdheden 40
      4.1.3. Besluit technische hulpmiddelen 40
      4.1.4. Internationale aspecten 41
      4.1.5. Wet politiegegevens 41
      4.1.6. Korte blik op de toekomst 43
      4.1.7. Conclusie 44
   4.2. Belastingdienst 44
      4.2.1. Inleiding 44
      4.2.2. Algemene bevoegdheden 45
      4.2.3. Bijzondere bevoegdheden Douane 47
      4.2.4. Bijzondere bevoegdheden FIOD-ECD 48
      4.2.5. Conclusie 49
   4.3. MIVD 50

4.3.1. Grondslag voor bevoegdheden 50
4.3.2. Bijzondere bevoegdheden 51
4.3.3. Eisen aan gebruik van bevoegdheden 52
4.3.4. Korte blik op de toekomst 53
4.3.5. Conclusie 53
5. Wet openbaarheid van bestuur 54
5.1. Inleiding 54
5.2. Bestuursorgaan 55
5.3. Documenten 55
5.4. Bestuurlijke aangelegenheid 57
5.5. Openbare informatie 57
5.6. Uitzonderingsgronden 58
5.6.1. Sectorwetgeving gaat voor Wob 58
5.6.2. Andere belangen dan openbaarheid prevaleren 59
5.6.3. Opsporingsbelang 59
5.6.4. Persoonlijke levenssfeer 60
5.6.5. Informatie ten behoeve van intern beraad 61
5.7. Conclusie 61

Deel II. Waarborgen

6. Privacymaatregelen in het systeemontwerp 63
6.1. Privacyrobuust ontwerpen (Privacy by Design) 63
6.2. Privacybeschermende technologieën (PETs) 64
6.2.1. Privacy-ontwerpprincipes 64
6.3. Conclusie 67
7. Transparantie en accountability 68
7.1. Inleiding 68
7.2. Begripsbepaling 68
7.3.1. Legitimiteit 68
7.3.2. Accountability 69
7.3.3. Vertrouwen 69
7.3. Het belang van transparantie 70
7.4 Accountability 72
7.5. Conclusie 74

Deel III. Conclusies en aanbevelingen

8. Conclusies en aanbevelingen 76
8.1. Conclusies ten aanzien van systeemontwikkeling en -beheer 76
8.1.1. Functionaliteiten van zoeken, bewerken en opslaan 76
8.1.2. Overige aspecten van systeemontwikkeling en -beheer 79
8.2. Conclusies ten aanzien van gebruik van het systeem 80
8.3. Afsluiting 82
9. Een privacychecklist voor HDIeF-tools 84

Bijlagen

1. HDIeF, iRN en iColumbo 87
1.1. Aanleiding 87
1.2. iRN 87
1.3. iColumbo 88
1.4. HDIeF 90
2. Onderzoeksbronnen 92
3. Samenstelling begeleidingscommissie 93
4. Literatuurlijst 94

Afkortingen

Awb	Algemene wet bestuursrecht
AWR	Algemene wet rijksbelastingen
CBP	College Bescherming Persoonsgegevens
EER	Europese Economische Ruimte
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
HDIeF	Herkenning Digitale Informatie en Fingerprinting
HR	Hoge Raad
ICT	informatie- en communicatietechnologie
iRN	Internet Research & Investigation Network
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NJ	*Nederlandse Jurisprudentie*
OPTA	Onafhankelijke Post- en Telecommunicatie Autoriteit
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
Rb.	Rechtbank
Wbp	Wet bescherming persoonsgegevens
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002
Wob	Wet openbaarheid van bestuur
WvSr	Wetboek van Strafrecht
WvSv	Wetboek van Strafvordering
T&C Sv	Tekst & Commentaar Strafvordering

Managementsamenvatting

iRN/iColumbo is een in ontwikkeling zijnde infrastructuur waarmee Nederlandse overheidsinstanties onderzoek kunnen doen in open Internetbronnen. Op deze infrastructuur kunnen diverse modules worden aangesloten, ontwikkeld binnen het programma HDIeF, om de resultaten van zoekacties te combineren, selecteren, bewerken en presenteren. Het onderhavige onderzoek analyseert of iRN/iColumbo als centrale infrastructuur en de binnen het programma HDIeF ontwikkelde modules voor deze infrastructuur in overeenstemming zijn met Nederlandse (en waar relevant Europese) wetgeving rond privacy en dataprotectie, auteursrechten en databankrechten, sectorale wetgeving betreffende eindgebruikers en de Wet openbaarheid van bestuur.

Aangezien iColumbo en de daarop aan te sluiten modules nog volop in ontwikkeling zijn, valt niet eenduidig te concluderen in welke mate ze aan bestaande wetgeving voldoen. Daarnaast is het moeilijk conclusies te trekken over de juridische *compliance* van de infrastructuur en modules, aangezien dat voor een belangrijk deel afhangt van het gebruik en de context van dat gebruik. Afhankelijk van de eindgebruiker zijn hierop immers verschillende juridische regimes van toepassing.

Tegelijk biedt deze situatie de mogelijkheid om de nu gemaakte of nog te maken ontwerp- en gebruikskeuzes mede te stoelen op de in dit rapport gesignaleerde juridische aandachtspunten en randvoorwaarden. Bij ontwerp, beheer en gebruik spelen persoonsgegevens en auteursrechten een belangrijke rol, primair met betrekking tot de gegevens die uit open Internetbronnen worden verzameld, maar secundair ook met betrekking tot gegevens over het systeem en zijn gebruikers zelf. Door tijdig oog te hebben voor deze juridische aspecten en maatregelen te nemen om aan wettelijke plichten te voldoen, kan worden geprobeerd de infrastructuur en modules en het gebruik daarvan zo privacyrobuust mogelijk te maken, volgens het principe van Privacy by Design. Bovendien wordt hiermee al in algemene zin geanticipeerd op het voldoen aan de (contextafhankelijke) toepasselijke wettelijke regimes. Die maatregelen zullen waar mogelijk moeten bestaan uit technische (en technisch-organisatorische) maatregelen (Privacy Enhancing Technologies), maar ook uit een adequaat stelsel van toezicht, auditing en andere accountability-faciliterende maatregelen.

Dit is geen eenvoudige opgave. Bij de te maken keuzes zullen diverse belangenafwegingen moeten worden gemaakt, niet alleen tussen juridische eisen enerzijds en operationele belangen anderzijds, maar ook tussen bepaalde juridische eisen op verschillende gebieden (bijvoorbeeld tussen plichten tot vernietiging van gegevens en plichten tot bewaring voor bewijsdoeleinden). Dit vereist een nadere bestudering van de precieze belangen die spelen en een intelligente en creatieve benadering om oplossingen te vinden die recht kunnen doen aan verschillende belangen tegelijk. Ook hierbij kunnen het gedachtegoed en de in ontwikkeling zijnde technische hulpmiddelen van Privacy by Design een productieve rol spelen.

De plicht om iRN/iColumbo in overeenstemming te brengen en houden met wetgeving is een gezamenlijke opdracht voor de systeemontwikkelaars, systeembeheersorganisatie en eindgebruikers. In een complex netwerk als het onderhavig mag de verantwoordelijkheid van individuele partijen niet ondersneeuwen doordat de verantwoordelijkheden binnen het netwerk niet expliciet zijn belegd. Het is essentieel dat alle bij iRN/iColumbo betrokken actoren zich gezamenlijk verantwoordelijk tonen en een gemeenschappelijke *governance*-structuur ontwikkelen, zowel voor het ontwikkel- en beheerproces als voor het gebruik van de infrastructuur en de daarop aan te sluiten tools.

De gemiddelde burger zal niet op de hoogte zijn van alle moderne technische mogelijkheden van openbrononderzoek en daarom ook niet (hoeven te) verwachten dat de overheid op grote schaal gebruik maakt van (intelligente combinaties van) gegevens uit open bronnen. Daarom is naast aandacht voor accountability (in de vorm van een adequate governance-structuur met voldoende *checks and balances*) ook transparantie van groot belang. De ontwikkeling van een infrastructuur met allerlei toegevoegdewaarde-functionaliteiten die door een breed spectrum aan overheidsinstanties zal worden gebruikt, moet kortom voldoende worden gelegitimeerd. De overheid, en in het bijzonder het primair verantwoordelijke departement, zal moeten kunnen beargumenteren waarom een systeem als iColumbo noodzakelijk is te ontwikkelen en te

gebruiken in onze democratische samenleving, en waarom de manier waarop het systeem is ingericht voldoet aan de algemene beginselen van subsidiariteit en proportionaliteit en aan juridische eisen van privacy en auteursrechten. Transparantie zowel over de infrastructuur en modules in het algemeen als over concreet gebruik hiervan (zodat de burger die geraakt wordt in zijn belangen daartegen in rechte kan opkomen) zal bijdragen aan het legitimeren van het systeem en daarmee aan de maatschappelijke acceptatie ervan.

1. Inleiding

1.1. Achtergrond: systemen voor openbrononderzoek door autoriteiten

Een steeds groter deel van het sociale leven in Nederland vindt plaats op het Internet. Veel communicatie, maar ook afspraken en sociale contacten lopen via sites als Facebook, Hyves en LinkedIn. Verder worden diensten als Twitter, YouTube en Flickr, evenals blogs en webfora, door steeds meer mensen gebruikt. Als gevolg hiervan kunnen opsporings- en handhavingsdiensten ook steeds vaker gebruik maken van deze media bij hun taakuitoefening.

Op dit moment hebben diverse handhavings- en opsporingsdiensten eigen tools ontwikkeld voor het doen van onderzoek op het Internet. Dit kunnen tools zijn waarbij Twitter uitgelezen worden of die een sociaal netwerk van een verdachte in kaart brengen. Dit laatste gebeurt echter ook nog vaak handmatig. Sommige handhavings- en opsporingsdiensten gebruiken echter ook commerciële producten, zoals Coosto,[1] die oorspronkelijk bedoeld zijn om het gebruik van merknamen in kaart te brengen.

Als gevolg van al deze eigen oplossingen van verschillende handhavings- en opsporingsdiensten, wordt er dubbel werk gedaan en mogelijk ook langs elkaar heen gewerkt. Bovendien heeft de ene dienst een goede technische oplossing voor een probleem waar de andere dienst nog steeds veel mankracht voor in moet zetten.

Binnen de politie is iRN (Internet Research & Investigation Network) ontwikkeld, waarbij opsporingsinstanties en overheidsdiensten met een toezichthoudende of controlerende wettelijke taak op een gecontroleerde manier het Internet kunnen gebruiken voor onderzoek, opsporing of 'surveillance'. iRN heeft hierin een ISP-functionaliteit: het biedt Internet en verschillende aanvullende diensten aan eindgebruikers. Zij kunnen zo het Internet op een veilige, forensisch geborgde manier gebruiken bij opsporing en onderzoek. Het is hierbij mogelijk om zowel 'zichtbaar' als 'onzichtbaar' op Internet onderzoek te doen. Alles wat de gebruiker op Internet ziet en doet wordt vastgelegd en kan gebruikt worden als bewijsmateriaal. Momenteel wordt het project ‘verduurzaamd’, zodat het niet langer bij een regionaal politiekorps is ondergebracht maar een zelfstandige positie krijgt.

Een volgende stap voor iRN is om naast de bestaande ISP-functionaliteit ook mogelijkheden voor systematisch openbronnenonderzoek te bieden. Hiervoor is het iColumbo-project gestart. iColumbo is een dienst voor iRN-gebruikers waarmee automatisch informatie van Internet wordt verzameld, geanalyseerd en op een 'slimme manier' gepresenteerd aan eindgebruikers. Hierdoor zien gebruikers per onderzoek de informatie die voor hen interessant is, zonder dat ze handmatig Internetinformatie moeten verzamelen en combineren. iColumbo maakt een analyseslag over informatie uit open bronnen, waarbij gegevens uit verschillende open bronnen worden gekoppeld en vergeleken, resultaten worden ontdubbeld, en zoekresultaten op een inzichtelijke manier worden gepresenteerd. Hierbij kan ook onderscheid gemaakt worden al naar gelang de rechten die de verschillende gebruikers hebben.

iColumbo is een platform waarin verschillende modules toegevoegd kunnen worden om de analyseresultaten van het systeem te verbeteren. Op dit moment wordt hierbij gebruik gemaakt van de Xtas-module, die meerdere soorten tekstuele analyses op data kan uitvoeren, en op basis waarvan verbanden tussen teksten kunnen worden gelegd en teksten onderling vergeleken kunnen worden. iColumbo kan hierdoor bijvoorbeeld sociale netwerken in kaart brengen. Door de modulaire opzet is het mogelijk om later extra modules toe te voegen, bijvoorbeeld voor socialenetwerkanalyse, video- en fotoherkenning en beeldanalyse.

De ontwikkeling van iColumbo wordt mede gefaciliteerd door het programma Herkenning Digitale Informatie en Fingerprinting (HDIeF) van de NCTV, waarin onderzoek gedaan wordt naar het inzetten van technieken voor het geautomatiseerd herkennen van digitale gegevens. Dit kan zijn in tekst, plaatjes, maar ook video’s en geluidsfragmenten. Binnen HDIeF worden modules ontwikkeld die aangesloten kunnen worden op iColumbo, om een integraal platform te creëren voor openbrononderzoek door de overheid. Een uitgebreidere beschrijving van iRN, iColumbo en HDIeF is te vinden in bijlage 1.

[1] http://www.coosto.nl.

iRN/iColumbo kan één overkoepelend platform vormen voor een breed scala aan eindgebruikers bij de Nederlandse overheid, zodat al deze eindgebruikers eenvoudig gebruik kunnen maken van dezelfde tools met uiteenlopende functionaliteiten. Iedere toegelaten eindgebruiker kan, afhankelijk van zijn rechten, gebruik maken van het platform. Het systeem logt elk gebruik en kent een terugspeelfunctie om integraal zoekvragen en antwoorden te kunnen terugzien, zodat gevonden materiaal bruikbaar is als bewijs in een rechtszaak.

1.2. Doelstelling en vraagstelling

De functionaliteit die in het iRN/iColumbo-raamwerk geïntegreerd wordt richt zich in eerste instantie op het verzamelen, selecteren en presenteren van gevonden informatie. Voor eindgebruikers zijn belangrijke functionaliteiten naam- of objectherkenning in tekstbestanden, een geautomatiseerde selectie van resultaten (bijvoorbeeld ontdubbeling) en een inzichtelijke presentatie, bijvoorbeeld door middel van visualisatie van netwerken tussen personen. Op de langere termijn wordt ook gedacht aan functionaliteit waarbij het systeem zelfstandig een analyse uitvoert en zelfstandig op zoek gaat naar extra informatie.

Gezien de hoeveelheid en aard van alle informatie die inmiddels op het Internet staat, is het mogelijk om veel informatie over burgers te verzamelen en met elkaar te verbinden. Daarbij kan een indringend beeld van de persoon ontstaan, dat overigens niet altijd een volledig of correct beeld hoeft te zijn in de context waarvoor een overheidsdienst de informatie verzamelt. Het systeem kan hierdoor een behoorlijke impact hebben op de privacy. Internetgebruikers zijn vaak niet bekend met de mogelijkheden die openbrononderzoek inmiddels biedt om informatie uit verschillende open bronnen met elkaar in verband te brengen, en zij zullen vaak ook niet direct verwachten dat instanties als de Belastingdienst of de politie systematisch informatie verzamelen van Internetbronnen. Dit betekent dat er een afbreukrisico bestaat voor het systeem, als bij de ontwikkeling en het gebruik ervan niet zorgvuldig wordt omgegaan met mogelijke privacybezwaren en eventuele andere juridische haken en ogen.

Tegen deze achtergrond is de **doelstelling** van het onderhavige onderzoek het doorlichten op juridische compliance van de door het programma HDIeF gefinancierde systemen voor openbrononderzoek, met name het project iColumbo en in het verlengde daarvan het iRN als centrale infrastructuur. Daarnaast beoogt het onderzoek een privacychecklist te ontwikkelen waarmee de privacybestendigheid van andere of toekomstige tools kan worden nagelopen.

De **vraagstelling** die centraal staat is: zijn de binnen het programma HDIeF ontwikkelde systemen (met name iColumbo en in het verlengde daarvan het iRN als centrale infrastructuur) privacybestendig en in overeenstemming met IE- en overige relevante wetgeving? Voor zover er lacunes of onduidelijkheden in de juridische bestendigheid zijn, welke waarborgen kunnen dan worden ingebouwd tegen onwenselijk gebruik of misbruik van de systemen en de daarin verwerkte informatie, gegeven de beoogde primaire eindgebruikers?

1.3. Afbakening

In dit onderzoek voeren we een juridische analyse op hoofdlijnen uit. We beperken ons daarbij tot het geldende Nederlandse recht, vanzelfsprekend met inachtneming van het Europeesrechtelijke kader waar relevant. De analyse beperkt zich tot de juridische aspecten die het belangrijkste zijn voor systeemontwikkelaars en eindgebruikers om rekening mee te houden; op basis van een quickscan van mogelijk relevante juridische aspecten, hebben wij gekozen voor behandeling van wetgeving rond privacy en bescherming van persoonsgegevens, auteursrecht en databankenrecht en de Wet openbaarheid van bestuur. We verwijzen kort naar aanhangige of voorgestelde wetswijzigingen voor zover die naar verwachting een significante impact kunnen hebben voor de juridische situatie. De analyse is juridisch van aard; we besteden geen aandacht aan ethische aspecten, behalve voor zover deze van invloed zouden kunnen zijn op de juridische (on)toelaatbaarheid bij de inkleuring van open normen.

We maken in het rapport onderscheid tussen ontwikkeling en beheer van het systeem enerzijds (ontwerpfase en onderhoud) en eindgebruik anderzijds. De nadruk in dit onderzoek ligt vanuit de onderzoeksvraag op het systeem zelf, maar aangezien de juridische aspecten van het systeem nauw verweven zijn met de context van het gebruik, en die context zeer verschillend is voor uiteenlopende typen eindgebruikers, wordt er ook aandacht besteed aan de juridische voorwaarden waaraan eindgebruikers moeten voldoen. Omdat dit niet mogelijk is te doen voor de

hele breedte van het eindgebruik, hebben wij ter illustratie drie eindgebruikers die vallen onder verschillende juridische regimes qua bevoegdheden en randvoorwaarden: de politie, de Belastingdienst en de MIVD voor het doen van screeningonderzoeken.

Bij het onderzoek gaan we uit van de functionaliteiten die momenteel in gebruik zijn of die op korte termijn worden voorzien: afscherming van het IP-adres van de zoeker, geautomatiseerd verzamelen en selecteren van gegevens, tekstanalyse, en presenteren van gegevens. Functionaliteiten als spraakherkenning, stemherkenning of gezichtsherkenning zijn buiten beschouwing gelaten, omdat naar verwachting niet op korte termijn modules met dergelijke functionaliteiten in het systeem worden geïntegreerd.

1.4. Methoden van onderzoek

Het onderzoek is uitgevoerd op basis van literatuuronderzoek, inclusief een wets- en jurisprudentieanalyse, interviews met betrokkenen en een workshop met eindgebruikers. Een overzicht van de interviews en workshopdeelnemers is te vinden in bijlage 2.

1.5. Leeswijzer

Het rapport bestaat uit twee delen. Deel I bevat ter beantwoording van het eerste deel van de onderzoeksvraag een juridische analyse van privacy en bescherming van persoonsgegevens (hfd. 2), auteursrecht en databankenrecht (hfd. 3), wetgeving met betrekking tot eindgebruikers (hfd. 4), en de Wet openbaarheid van bestuur. Deel II bevat ter beantwoording van het tweede deel van de onderzoeksvraag een nadere reflectie op mogelijke waarborgen voor juridische compliance van iRN/iColumbo. Dit betreft maatregelen in de vorm van technisch-organisatorische mogelijkheden om compliance te ondersteunen of af te dwingen (het concept ‘privacy by design’, hfd. 6) en maatregelen die transparantie en accountability verhogen (hfd. 7). Hoofdstuk 8 bevat een conclusie in de vorm van een dwarsdoorsnede van juridische aandachtspunten waarbij bij de verschillende onderdelen van iRN/iColumbo rekening mee moet worden gehouden. Aansluitend volgt een privacychecklist waarmee de privacybestendigheid van andere of toekomstige tools kan worden nagelopen. De bijlagen bevatten een nadere beschrijving van iRN/iColumbo en van de onderzoeksmethoden en -bronnen.

Deel I. Juridische aspecten

In dit deel gaan we in op het eerste deel van de onderzoeksvraag:

> zijn de binnen het programma HDIeF ontwikkelde systemen (met name iColumbo en in het verlengde daarvan het iRN als centrale infrastructuur) privacybestendig en in overeenstemming met IE- en overige relevante wetgeving?

Naast privacy en bescherming persoonsgegevens (hfd. 2) en IE-recht (hfd. 3) blijkt ook de wetgeving voor eindgebruikers van groot belang te zijn voor de compliance-vraag, daarom wordt daar ook aandacht aan besteed voor de drie gekozen eindgebruikers (hfd. 4). Tevens moet rekening worden gehouden met de Wet openbaarheid van bestuur (hfd. 5).

2. Privacy en bescherming van persoonsgegevens

2.1. Inleiding

Dat systemen voor openbrononderzoek de verwerking van persoonsgegevens met zich brengen is naast een specifiek doel ook een onvermijdelijk neveneffect. Hiermee wordt bedoeld dat zelfs indien een openbrononderzoek zich niet richt op identificeerbare personen, het niet valt uit te sluiten dat in een dergelijk onderzoek persoonsgegevens verwerkt zullen worden; de definitie van persoonsgegevens wordt heden ten dage zeer ruim uitgelegd. Systemen zijn over het algemeen niet toegerust om onderscheid in typen gegevens te maken. Dit is ook het geval bij iRN/iColumbo; momenteel kan het systeem geen onderscheid maken tussen bijvoorbeeld auteursrechtelijk beschermde data, persoonsgegevens en gevoelige gegevens.[2]

Bij openbrononderzoek spelen vanuit juridisch perspectief nog een aantal andere kenmerkende aspecten. In de eerste plaats zal het openbrononderzoek zich niet beperken tot territoriale grenzen. Zelfs al zou het technisch mogelijk zijn een zoekopdracht te begrenzen tot een bepaald territoriaal gebied, dan zal het doel van de zoekopdracht veelal juist mede gelegen zijn in het ontdekken van informatie afkomstig uit verschillende territoriale gebieden. Niet voor niets wordt bij de functionaliteiten van systemen voor openbrononderzoek mede de aandacht gevestigd op vertaalmogelijkheden. Dit betekent overigens niet alleen dat gegevens op verschillende plaatsen gevonden kunnen worden; er bestaan, bijvoorbeeld via cloud computing, ook mogelijkheden om gevonden gegevens op verschillende plaatsen op te slaan. Als dit laatste het geval is, kan de verwerking van persoonsgegevens onderworpen zijn aan verschillende juridische regimes. In het kader van iRN/iColumbo is vastgesteld dat alle data worden opgeslagen in een centrale server. Dit vanuit het het doel om de verkregen informatie als bewijs te kunnen gebruiken. In dit rapport wordt ervan uitgegaan dat de opslag van de gegevens op Nederlands grondgebied plaatsvindt. Ook wordt uitgegaan van de situatie waarin degene die verantwoordelijk is voor de verwerking van persoonsgegevens (zie over de verantwoordelijke par. 2.3), gevestigd is op Nederlands grondgebied en dus gebonden is aan de in Nederland geldende wetgeving.

Voor privacy geldt een ander regelgevend kader dan met betrekking tot gegevensbescherming. Hieronder zal eerst kort worden ingegaan op het regelgevend kader betreffende privacy, waarna meer uitgebreid wordt ingegaan op het wettelijk kader betreffende persoonsgegevens, dat gebaseerd is op drie Europese Richtlijnen. Deze richtlijnen zijn Richtlijn95/46/EG welke de algemene Richtlijnbetreffende gegevensverwerking is (kortweg de Dataprotectierichtlijn), Richtlijn2002/58/EG betreffende de verwerking van persoonsgegevens in de elektronische communicatiesector (E-privacyrichtlijn), en Richtlijn2006/24/EG betreffende dataretentie.[3]

In deze rapportage worden met het oog op privacy en gegevensbescherming twee gebruikersperspectieven onderscheiden. In de eerste plaats het perspectief van de persoonsgegevensverwerking die plaatsvindt in het kader van de ontwikkeling en het beheer van de systemen voor openbrononderzoek. Vanuit dit perspectief is met name de algemene Dataprotectierichtlijn van belang, die in Nederland geïmplementeerd is in de Wet bescherming persoonsgegevens (Wbp). Wanneer we gaan kijken naar het eindgebruik van de systemen voor openbrononderzoek, dan ligt een groot deel in de sfeer van politie en justitie en zal de verwerking van persoonsgegevens in dit kader veelal vallen buiten de werkingssfeer van de Wbp, maar

[2] Interview Corné van der Sloot.

[3] Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Zie PubEG Nr. L 281 van 23/11/1995, p. 0031 – 0050. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), PubEG L 201 van 31.7.2002,, p. 37–47. Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, PubEG Nr. L 105 van 13/04/2006, p. 0054 – 0063.

binnen de werkingssfeer van het Kaderbesluit 2008/977/JBZ, dat in Nederland geïmplementeerd is in de Wet politiegegevens (zie par. 4.1.5) en de Wet justitiële en strafvorderlijke gegevens.[4]

iRN/iColumbo is nog volop in ontwikkeling, waardoor de exacte functionaliteit nog niet vaststaat. De functionaliteit waar het onderzoek zich met name op richt betreft enerzijds zoekacties die zich niet specifiek op een persoon richten maar worden gebruikt voor het in kaart brengen van bredere tendensen, en anderzijds wat wel genoemd wordt Person-of-interest-profiling (Poip), hetgeen momenteel alleen geschiedt door eindgebruikers in het kader van opsporings- en handhavingstaken. De gebruiker kan bij dit laatste een naam ingeven, waarna het systeem de crawlers aanzet en data verzamelt en analyseert. Hierbij is het van belang dat de resultaten van Poip multimediaal zijn. Andere mogelijke toekomstige functionaliteiten worden wel overwogen, zoals het proberen om crimineel gedrag vooraf te herkennen, bijvoorbeeld door gedragsprofilering. Aangezien dit geen bestaande of op korte termijn ingebouwde functionaliteiten betreft, laten we deze buiten beschouwing in dit rapport.

Vooralsnog wordt uitgegaan van een systeem waarbij data periodiek verzameld worden. Een zoekvraag heeft altijd een bepaalde duur, waarbij aangegeven wordt hoe vaak de zoekactie uitgevoerd moet worden. Vooralsnog worden in het kader van iRN/iColumbo alle data altijd gekoppeld aan een specifiek project, waarbij per project gespecificeerd is dat alleen de gebruikers betrokken in dat project en afhankelijk van hun rol in dat project, toegang hebben tot de data. Uit de interviews blijkt dat tussen gebruikersprojecten wel bepaalde basale data uitgewisseld worden. Vanuit het perspectief van privacy en gegevensverwerking gaat het hier ofwel om verenigbaar gebruik, ofwel om een nieuwe verwerking die als zodanig getoetst moet worden op verenigbaarheid met het juridische raamwerk.

2.2. Privacy: art. 10 Gw en art. 8 EVRM

2.2.1. Privacy en gegevensbescherming

In de eerste plaats is het belangrijk de concepten privacy en gegevensbescherming te begrijpen. Privacy en gegevensbescherming zijn gerelateerde begrippen maar vallen niet samen. Privacy is een overkoepelend begrip, een fundamenteel recht dat nauw verbonden is met persoonlijke vrijheid. Onder het overkoepelende begrip privacy kunnen verschillende dimensies worden onderscheiden. Zo is er een recht op lichamelijke integriteit, het recht om zelf te bepalen met wie men al dan niet relaties aan wil gaan en de bescherming van de ruimte waarin men zich bevindt, zoals het huisrecht. Als een vierde dimensie kan gewezen worden op de zogenaamde informationele privacy, ofwel het recht op gegevensbescherming. Privacy is dus een begrip dat verschillende deelaspecten of dimensies omvat: lichamelijke, relationele, ruimtelijke en informationele. Door de enorme toename in de (geautomatiseerde) verwerking van persoonsgegevens en de grote aandacht die de informationele privacydimensie daardoor is gaan genieten, wordt privacy soms ten onrechte vereenzelvigd met gegevensbescherming. Bescherming van persoonsgegevens maakt deel uit van het ruimere begrip privacy, maar heeft daarnaast ook een zelfstandige betekenis; bovendien heeft een deel van gegevensbescherming als zodanig niet zozeer met privacy te maken, als wel met basale fatsoensnormen of ‘datahygiëne’ voor de omgang met persoonsgegevens, die evenzeer gelden wanneer een gegeven niet (in een bepaalde context) privacygevoelig is.

Het belang vann het maken van onderscheid tussen privacy en gegevensbescherming is gelegen in het feit dat beide rechten een eigen wettelijk regime kennen. Wanneer vaststaat dat de privacy van een individu is geschonden, hoeft dit niet te betekenen dat dit komt doordat onrechtmatig met persoonsgegevens is gehandeld, de schending kan ook verband houden met een van de andere privacydimensies.

[4] Wet van 6 oktober 2011 tot wijziging van de Wet politiegegevens en van de Wet justitiële en strafvorderlijke gegevens in verband met de implementatie van het kaderbesluit van de Raad van de Europese Unie 2008/977/JBZ over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken en de implementatie van het Besluit van de Raad 2009/371/JBZ van 6 april 2009 tot oprichting van de Europese politiedienst (Europol), *Staatsblad* 2011, nr. 490.

2.2.2. Het recht op privacy, Handvest en EVRM

Voor Europa is de belangrijkste bepaling betreffende het recht op privacy artikel 8 van het Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (EVRM). Daarnaast is het recht op privacy opgenomen in het Handvest van de Grondrechten van de Europese Unie, dat met de inwerkingtreding van het Verdrag van Lissabon op 1 december 2009[5] bindend is geworden voor de Unie en de lidstaten.[6] Bijzonder aan het Handvest is dat naast het algemene recht op privacy ook het recht op gegevensbescherming in een eigen artikel is vastgelegd.

Artikel 7 Handvest betreft de eerbiediging van het privé-leven en het familie- en gezinsleven. Dit artikel luidt: 'Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.' Artikel 8 betreft de bescherming van persoonsgegevens en luidt:

> 1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
>
> 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet.
>
> Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
>
> 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Hoewel er jarenlang in de juridische literatuur discussie is geweest over de vraag of het recht op gegevensbescherming wel of geen fundamenteel recht is, of zou moeten zijn, is met de inwerkingtreding van het Verdrag van Lissabon in ieder geval voor de Europese Unie deze discussie beslecht met als uitkomst dat gegevensbescherming inderdaad als een mensenrecht erkend is. Ondanks de verankering van privacy en gegevensbescherming in het Handvest, zal artikel 8 EVRM van groot belang blijven voor de EU. Dit komt in de eerste plaats omdat het Handvest beoogt de grondrechten van personen te beschermen tegen regelgeving van de instellingen van de Unie en van de lidstaten wanneer zij de Verdragen van de Unie toepassen. Artikel 8 EVRM is vooral bedoeld om burgers te beschermen tegen de overheid, maar bovendien is in de rechtspraak erkend dat artikel 8 EVRM ook gelding heeft in private relaties (bijvoorbeeld tussen bedrijven en consumenten). De uitleg van het recht op privacy door het Europees Hof van de Rechten van de Mens zal over het algemeen leidend zijn en blijven binnen de EU. Doordat Nederland is aangesloten bij het EVRM moet ook artikel 10 van de Nederlandse Grondwet worden uitgelegd in het licht van artikel 8 EVRM. Deze paragraaf baseert zich daarom verder op dit artikel.

Artikel 8 van het EVRM betreffende het Recht op eerbiediging van privé-, familie- en gezinsleven, luidt:

> 1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
>
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Uit deze bepaling is een gelaagde privacytoets af te leiden, die uiteenvalt in de volgende vragen: Is er sprake van een inbreuk op de privacy? Zo ja, is deze gerechtvaardigd? Hiertoe moet eerst bekeken worden of de inmenging op het recht op privacy voorzien is bij de wet. Vervolgens moet gekeken worden of een van de in artikel 8 genoemde belangen met de inbreuk gediend wordt. Zoals blijkt uit de laatste regel van artikel 8 kan hier sprake zijn van een belangenafweging tussen het recht op privacy van het individu en de rechten en vrijheden van anderen. Tot slot moet getoetst worden of de schending 'noodzakelijk is in een democratische samenleving'. Dit criterium wordt uitgelegd aan de hand van het beginsel van proportionaliteit en subsidiariteit. Proportionaliteit betekent dat de privacy-inbreukmakende maatregel in verhouding moet staan tot het doel dat men wil bereiken. Subsidiariteit houdt in dat bij een keuze uit verschillende middelen, het minst ingrijpende middel ingezet moet worden.

---

5 Zie http://europa.eu/lisbon_treaty/full_text/index_nl.htm.
6 Zie http://www.europarl.europa.eu/charter/pdf/text_nl.pdf.

Met het oog op iRN/iColumbo is in de eerste plaats relevant dat het systeem als zodanig mogelijk al beschouwd kan worden als een systeem dat inbreuk op de privacy maakt. De enkele wetenschap bij burgers dat de overheid systemen als iRN/iColumbo inzet voor onderzoek in open bronnen kan hen immers het gevoel geven dat zij 'bekeken' worden, waarop zij mogelijk hun gedrag gaan aanpassen en minder onbevangen zichzelf zullen zijn, bijvoorbeeld binnen online sociale netwerken. Dit kan gezien worden als een inbreuk op de privacy. Uit de test van artikel 8 EVRM volgt dan de volgende aspecten onderbouwing behoeven.

1. Aangeven in welke wet de inbreuk op het recht op privacy is voorzien.
2. Aangeven met het oog op welk in artikel 8 genoemd belang de inbreuk plaatsvindt.
3. Aantonen waarom iRN/iColumbo noodzakelijk zijn in onze democratische samenleving.
4. Aantonen dat de systemen het doel waarvoor ze ontwikkeld worden daadwerkelijk bereiken in dat het middel in verhouding staat tot dit doel.
5. Aantonen dat dit doel niet met minder ingrijpende middelen bereikt kan worden.

2.3. Wet bescherming persoonsgegevens

2.3.1. Toepasselijkheid Wbp

Alvorens de inhoud van het regime van gegevensverwerking aan de hand van de Wbp nader uit te leggen, is het van belang om vast te stellen in welke gevallen de Wbp van toepassing is. De toepasselijkheid van de Wbp moet worden bepaald aan de hand van de eerste vier artikelen van de Richtlijn. Zoals al eerder opgemerkt is dit in het kader van de onderhavige studie zeer relevant omdat de eindgebruikers van de systemen voor openbrononderzoek mogelijk aan een ander juridisch regime onderworpen zullen zijn dan de ontwikkelaars en beheerders van het systeem. Een en dezelfde partij kan overigens aan verschillende regimes onderworpen zijn doordat het doel van het openbron gebruik mede bepalend is voor de toepasselijkheid van een bepaald juridisch regime. De Wbp is bijvoorbeeld niet van toepassing op de verwerking van persoonsgegevens *ten behoeve van de politietaak.* Echter indien een politieagent niet ten behoeve van de politietaak persoonsgegevens verwerkt, kan de Wbp van toepassing zijn. Voor de eindgebruikers geldt dat een aantal van hen meestal niet zullen vallen onder het Wbp-regime, terwijl dit op andere eindgebruikers, zoals de Belastingdienst of sectorale toezichthouders, wel van toepassing zal zijn. Aangezien bij de ontwikkeling en het beheer van het iColumbo-systeem gebruik gemaakt zal worden van werkelijke data, en ook in dit verband dus sprake zal zijn van de verwerking van persoonsgegevens, is het Wbp-regime ook hierop van toepassing.

De eerste vier artikelen van de Wbp betreffen de toepasselijkheid en reikwijdte van deze wet. De Wbp bepaalt onder welke voorwaarden persoonsgegevens mogen worden verwerkt en wat daarbij de regels zijn. Voor de toepasselijkheid van deze wet moet dus sprake zijn van 'verwerking van persoonsgegevens', hetgeen gedefinieerd wordt in artikel 1 sub a en b van de Wbp:

> a) persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
>
> b) verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

In de Wbp wordt een niet-limitatieve opsomming gegeven van handelingen met betrekking tot persoonsgegevens die vallen onder het begrip verwerking. Er bestaat consensus dat dit begrip ruim moet worden uitgelegd, waardoor eigenlijk elke handeling, van creatie tot en met de vernietiging van gegevens, binnen de reikwijdte van de term 'verwerking' valt. Hoewel *data mining* dus niet expliciet genoemd wordt in de definitie van verwerking, valt dit wel degelijk binnen het concept verwerking.

De consensus over het begrip verwerking bestaat niet ten aanzien van de reikwijdte van het begrip 'persoonsgegeven'. Er is bijvoorbeeld discussie over de vraag of een IP-adres al dan niet een persoonsgegeven is. In Europa is de zogenaamde 'Groep Gegevensbescherming Artikel 29' (hierna: Artikel 29 Werkgroep) belast met het streven naar een homogene uitleg van het Europese juridische kader betreffende gegevensbescherming. Hiertoe brengen zij opinies uit die

nader ingaan op de wijze waarop de Richtlijn uitgelegd en toegepast moet worden.[7] Over het begrip 'persoonsgegeven' heeft de groep al meerdere keren advies uitgebracht, het meest omvangrijk in een opinie uit 2007.[8] Dit laat zien dat het niet evident is in welke gevallen een gegeven is aan te merken als 'een gegeven dat een natuurlijk persoon identificeert of mogelijk kan identificeren'. Uit de adviezen blijkt wel duidelijk een trend om het begrip persoonsgegevens ruim uit te leggen; zelfs als het niet zeker is of identificatie mogelijk is, moet soms toch uitgegaan worden van persoonsgegevens, zoals bijvoorbeeld blijkt uit een advies over IP-adressen. In een Internet-café is het voor Internetdienstverleners niet altijd mogelijk om te weten of het IP-adres in kwestie identificatie mogelijk maakt. Toch stelt de artikel 29 Werkgroep dat ook deze IP-adressen als persoonsgegevens behandeld moeten worden (tenzij de Internetdienstverlener met absolute zekerheid gegevens van niet-identificeerbare gebruikers kan onderscheiden). Meestal zal hij dan alle IP-informatie voor de zekerheid als persoonsgegevens moeten behandelen.[9]

Als we deze redenering breder doortrekken, dan zal onderzoek in open bronnen altijd, zelfs als het niet beoogd is, de verwerking van persoonsgegevens met zich brengen. Of de Wbp van toepassing is op deze verwerking is echter afhankelijk van de toepassing en reikwijdte van deze wet, die bepaald is in artikel 2 Wbp:

> 1. Deze wet is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij het onderzoek in open bronnen gaat het met name om geautomatiseerde verwerking van persoonsgegevens en, voor zover sommige handelingen in het proces niet automatisch uitgevoerd zullen worden, zal de relevante informatie in bestanden worden opgenomen, waarmee aan de eerste voorwaarde voor toepasselijkheid van de Wbp is voldaan. In artikel 2 en 3 Wbp worden echter ook enkele uitzonderingen genoemd:

> 2. Deze wet is niet van toepassing op verwerking van persoonsgegevens:
>
> a. ten behoeve van activiteiten met uitsluitend **persoonlijke of huishoudelijke doeleinden**;
>
> b. door of ten behoeve van **de inlichtingen- en veiligheidsdiensten**, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002;
>
> c. ten behoeve van de uitvoering van de **politietaak**, bedoeld in de artikelen 2 en 6, eerste lid, van de Politiewet 1993;
>
> d. die is geregeld bij of krachtens de **Wet gemeentelijke basisadministratie persoonsgegevens**;
>
> e. ten behoeve van de uitvoering van de **Wet justitiële en strafvorderlijke gegevens** en
>
> f. ten behoeve van de uitvoering van de **Kieswet**.
>
> 3. Deze wet is niet van toepassing op verwerking van persoonsgegevens door de **krijgsmacht** indien Onze Minister van Defensie daartoe beslist met het oog op de inzet of het ter beschikking stellen van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde. Van de beslissing wordt zo spoedig mogelijk mededeling gedaan aan het College.

De eerste uitzondering is in het kader van onderzoek in open bronnen door zowel de ontwikkelaars van het systeem als de voorziene eindgebruikers niet relevant. De verwerking van persoonsgegevens binnen iRN/iColumbo is immers niet van 'puur persoonlijke of huishoudelijke aard'. Met het oog op eindgebruikers zijn de uitzonderingen onder b), c), e) en f) wel relevant, aangezien de Wbp niet van toepassing is op de verwerking van persoonsgegevens door of ten behoeve van de inlichtingen- en veiligheidsdiensten, de politietaak, de uitvoering van de Wet justitiële en strafvorderlijke gegevens en de krijgsmacht. Veel van de voorziene eindgebruikers van de systemen voor openbrononderzoek die in dit rapport centraal staan zullen vallen binnen een van deze uitzonderingen. Voor deze verwerkingen geldt een speciaal regime van gegevensverwerking dat in specifieke wetgeving is ondergebracht. Met het oog op de drie

[7] De artikel 29 Werkgroep is in het leven geroepen door artikel 29 van de Dataprotectie Richtlijn, en heeft met name als taak het adviseren van de Europese Commissie over de uniforme toepassing (tevens interpretatie) en uitvoering van de Richtlijn, en in het algemeen over het niveau van databescherming binnen de Europese Unie. Zie ook artikel 30 Databescherming richtlijn.
[8] Groep gegevensbescherming artikel 29 2007.
[9] Ibid., p. 18.

partijen die in het kader van dit onderzoek nader belicht worden, geldt dat alleen voor de Belastingdienst de Wbp relevant zal zijn; voor de politie en voor de MIVD geldt een specifiek wettelijk regime (de Wet politiegegevens resp. art. 12 t/m 16 Wiv 2002).

Verder bestaat nog een uitzondering in artikel 3 van de Wbp voor verwerking voor uitsluitend journalistieke, artistieke of literaire doeleinden, die niet relevant is voor dit rapport.

Een laatste toets of de Wbp van toepassing is, ligt besloten in artikel 4, waarin het gaat om toepasselijk recht. Hoewel vaak gedacht wordt dat de locatie van *gegevens* bepalend is voor het antwoord op de vraag welk nationaal regime betreffende gegevensbescherming van toepassing is, gaat het Europese regime uit van de *vestigingsplaats* van degene die verantwoordelijk is voor de verwerking van persoonsgegevens. Met vestiging wordt bedoeld de zetel van de rechtspersoon en niet de locatie van de IT-faciliteiten die voor de verwerking van persoonsgegevens worden gebruikt. Wij gaan er in dit rapport van uit dat de eindgebruikers in Nederland gevestigd zijn, zodat de Wbp (behoudens bovengenoemde uitzonderingen) van toepassing is.

2.3.2. De begrippen 'verantwoordelijke' en 'bewerker'

Een centraal begrip in de Wbp is 'verantwoordelijke'. Artikel 1 d van de Wbp definieert 'voor de verwerking verantwoordelijke' als volgt:

> de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Het is niet ongebruikelijk dat een verantwoordelijke voor de feitelijke verwerking van persoonsgegevens andere partijen inschakelt. In de terminologie van de Wbp gaat het hierbij om 'bewerkers' (Richtlijn 95/46/EG spreekt van verwerker). Artikel 1 e van de Wbp definieert 'bewerker' als:

> degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Het grote verschil bestaat erin dat de bewerker niet het doel en de middelen voor de verwerking van persoonsgegevens bepaalt, maar slechts in opdracht van de verantwoordelijke persoonsgegevens verwerkt. Degene op wie een persoonsgegeven betrekking heeft, wordt 'betrokkene' genoemd.

In de Wbp is de relatie tussen verantwoordelijke, bewerker en derden[10] nader toegelicht in artikel 12 dat bepaalt:

> Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen.

Voor deze personen geldt een plicht tot geheimhouding van de gegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Artikel 14 van de Wbp betreft de plicht om de uitvoering van verwerkingen door een bewerker te regelen in een overeenkomst. De onderdelen van de overeenkomst die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen, worden schriftelijk vastgelegd. Voorts bepaalt dit artikel dat de verantwoordelijke zorg draagt dat de bewerker persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13 (beveiligingsplicht). Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt. Op grond van artikel 15 Wbp moet de verantwoordelijke bovendien zorg dragen dat de bewerker de verplichtingen uit de artikelen 6 tot en met 12 en 14 van de Wbp naleeft.

Niet in alle gevallen is duidelijk welke partij welke rol(len) vervult in de verwerking van persoonsgegevens. Wat die rollen zijn, kan per situatie verschillen. Als we de Belastingdienst als

10 In artikel 1 g Wbp gedefinieerd als: "ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken."

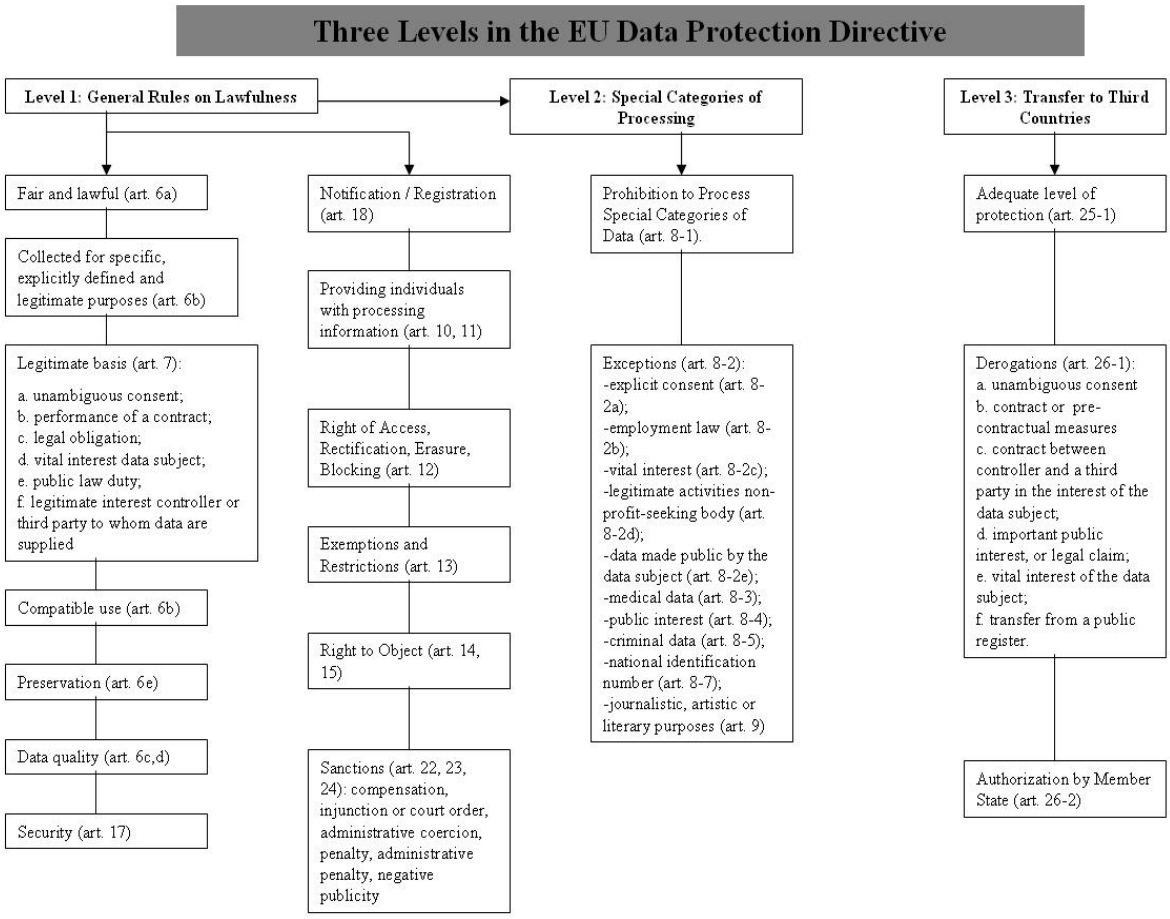
voorbeeld nemen, dan kunnen drie verschillende diensten onderscheiden worden die alle drie met een ander doel hetzelfde middel (iRN/iColumbo) in kunnen zetten voor onderzoek in open bronnen. Hierbij zal het van de organisatiestructuur van de Belastingdienst afhangen of de Belastingdienst als overkoepelend orgaan als verantwoordelijke te gelden heeft, of de afzonderlijke diensten, Belastingdienst Blauw, Douane en FIOD. Bij de afzonderlijke diensten wordt overigens niet gesproken van bewerkers, hierbij gaat het echt om externe partijen die worden ingeschakeld in het proces van gegevensverwerking. Wanneer binnen een en dezelfde organisaties verschillende partijen in dit proces betrokken zijn wordt gesproken van intern beheer. Bij intern beheer is sprake van een hiërarchische relatie ten opzichte van de verantwoordelijke, hetgeen niet het geval is bij een (externe) bewerker.

2.3.3. Een gelaagd systeem van gegevensbescherming

Nadat op basis van de eerste vier artikelen van de Wbp de toepasselijkheid van de wet is vastgesteld en wat de rol van de verantwoordelijke is, geeft het navolgende inzicht in wat inhoudelijk de consequenties zijn van de toepasselijkheid van de Wbp. Het Europees juridische raamwerk betreffende de verwerking van persoonsgegevens bestaat uit vijf lagen, waarvan de eerste drie zijn terug te vinden in Richtlijn 95/46/EG. In Nederland zijn deze drie lagen verankerd in de Wbp. De vijf lagen van het raamwerk zijn:

1. algemene regels voor de rechtmatigheid van de verwerking van persoonsgegevens;
2. regels voor de verwerking van bijzondere (gevoelige) gegevens;
3. regels betreffende de doorgifte van gegevens naar derde landen (landen buiten de EU);
4. sectorspecifieke wet- en regelgeving (waaronder de ePrivacyrichtlijn en de dataretentierichtlijn, maar ook nationale sectorspecifieke wetgeving zoals de Wet Geneeskundige BehandelingsOvereekomst;
5. onderliggende (contractuele) rechtsverhoudingen.

Van belang is dat deze lagen elkaar aanvullen. Indien bijzondere persoonsgegevens (zoals gegevens over etnische afkomst of gezondheid) verwerkt worden, dan zijn zowel de bepalingen uit de eerste laag als die uit de tweede laag van toepassing. Als deze bijzondere gegevens vervolgens ook nog doorgegeven worden aan een derde land, dan is bovendien ook laag 3 van toepassing. Bovendien moet per geval altijd bekeken worden of er sprake is van toepasselijke sectorspecifieke wetgeving, en of er wellicht binnen de rechtsverhouding contractuele afspraken zijn gemaakt die van invloed zijn op de wijze waarop gegevens al dan niet rechtmatig verwerkt mogen worden. Figuur 1 geeft een goed overzicht van deze drie lagen; deze zijn geënt op de bepalingen uit de Richtlijn, maar omdat Nederland de Richtlijnzeer nauwgezet heeft omgezet in het nationale recht, wijkt de Wbp slechts marginaal af van de Richtlijn.



Figuur 1: De drie lagen in de Dataprotectierichtlijn

Laag 1: Algemene bepalingen

Artikel 6 Wbp bepaalt dat persoonsgegevens worden verwerkt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze. Wat precies een 'behoorlijke en zorgvuldige wijze' is, wordt vervolgens uitgelegd in de artikelen die volgen op artikel 6. In de eerste plaats mogen gegevens alleen verzameld worden voor **welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden** (art. 7). Degene die doel en middelen vaststelt, moet deze doelen dus expliciet, compleet en duidelijk beschrijven. Voor zover de verwerking van persoonsgegevens wordt uitbesteed aan een bewerker, zal de doelomschrijving in de overeenkomst tussen verantwoordelijke en bewerker opgenomen moeten worden.

De verantwoordelijke moet niet alleen zorg dragen voor een deugdelijke vaststelling van het doel, maar zal tevens moeten garanderen dat gegevens niet worden verwerkt op een wijze die onverenigbaar is met de vastgestelde doeleinden (Art. 9). (Verdere verwerking van de gegevens is wel toegestaan voor historische, statistische of wetenschappelijke doeleinden; dat is hier verder niet relevant.) Artikel 9 bepaalt voorts dat verwerking van persoonsgegevens niet is toegestaan wanneer sprake is van een geheimhoudingsplicht op basis van ambt, beroep (bijv. arts) of wettelijk voorschrift. Over de precieze uitleg van artikel 9 bestaat discussie, die relevant is voor het zoeken van informatie in open bronnen. Indien persoon A informatie plaatst op laten we zeggen zijn openbare profielpagina bij Facebook, dan doet hij dit met als doel vindbaar te zijn voor anderen binnen de Facebook-gemeenschap. Hij doet dit echter niet om gevonden te worden door gebruikers van iRN/iColumbo. Een redenering zou dan kunnen zijn dat de verwerking van de gegevens in het kader van iRN/iColumbo in strijd is met artikel 9 van de Wbp; het doel van iColumbo-verwerking wijkt immers af van het doel van de Facebook-verwerking door de gebruiker. In een andere lezing van artikel 9 gaat het hier echter om elkaar opvolgende verwerkingen van gegevens. Dan moet de verwerking van degene die iRN/iColumbo gebruikt los worden gezien van de verwerking van degene die de gegevens in eerste instantie op Facebook

geplaatst heeft. De verwerking met iRN/iColumbo vormt een nieuwe zelfstandige verwerking. Wij volgen in dit rapport deze tweede interpretatie van artikel 9, waarin verenigbaar gebruik betrekking heeft op de verenigbaarheid van twee verwerkingen van één verantwoordelijke. Wij baseren deze uitleg op de Memorie van Toelichting bij de Wbp, die niet uitblinkt in helderheid, maar waarin consequent gesproken wordt van 'verenigbaar met het doel waarvoor gegevens verzameld/verkregen zijn'. Er wordt hierbij een passage gewijd aan profilering:

> Van belang in laatstgenoemd geval is vooral dat de gegevens buiten de betrokkene om zijn verkregen en deze gegevens bovendien zijn verwerkt tot een specifiek voor die persoon geldend profiel zonder deze persoon daarbij op enigerlei wijze te betrekken. Onder die omstandigheden zal veel eerder van onverenigbaarheid sprake zijn. Zijn daarentegen de gegevens van de betrokkene zélf verkregen en worden er bovendien met het oog op het belang van de betrokkene passende waarborgen geboden, is de kans groter dat aan de voorwaarde van verenigbaar gebruik is voldaan.[11]

Uit de context blijkt dat ook in dit citaat uitgegaan wordt van de verenigbaarheid van het oorspronkelijke doel waarvoor de verantwoordelijke de gegevens verkregen heeft met het opvolgende doel van profilering, en niet de verenigbaarheid van profilering met het oorspronkelijke doel van de betrokkene om informatie in open bronnen te plaatsen. Dit betekent dat artikel 9 hier relevant is voor het bepalen of het verder verwerken (zoals bewerken, selecteren en visueel presenteren) van gegevens die via iColumbo worden verzameld verenigbaar is met het doel van de verzameling.

Een ander punt om iRN/iColumbo in relatie te brengen tot artikel 9 Wbp betreft het gebruik van *crawl extender*. Het crawlen werkt in dit verband op basis van door de gebruiker aangegeven crawlvragen, waarbij een module in iRN/iColumbo de mogelijkheid biedt dat deze zelf het gecrawlde materiaal analyseert en op basis hiervan de crawlvragen uitbreidt. Dit gebeurt zonder verdere menselijke tussenkomst, maar leidt, op basis van de eerste zoekvragen, wel tot verdere en nieuwe verwerkingen van persoonsgegevens. Of dit mogelijk is hangt af van de vraag of dit verdere zoeken verenigbaar is met het oorspronkelijke doel. Dit stelt eisen aan de verantwoordelijke om het oorspronkelijke doel dusdanig te specificeren dat het voldoet aan de vereisten van doelspecificatie, maar voldoende ruimte biedt om met *crawl extender* gegenereerde zoekopdrachten te brengen binnen het bereik van verenigbaar gebruik.

Naast een gespecificeerd doel betreft een tweede belangrijke voorwaarde voor de verwerking van persoonsgegevens de aanwezigheid van een **legitieme verwerkingsgrond**. De rechtmatige verwerkingsgronden zijn limitatief opgesomd in artikel 8. De eerste verwerkingsgrond, 'toestemming van betrokkenen' (artikel 8 a Wbp) is praktisch gezien geen optie, voor systeemontwikkelaars en –beheerders noch voor eindgebruikers. Er is ook geen sprake van een verwerking die noodzakelijk is ter nakoming van een contractuele verplichting (artikel 8 b Wbp). Ook het vitaal belang van een betrokkene of derde (artikel 8 d Wbp) is voor ontwikkelaars en eindgebruikers geen toepasselijke verwerkingsgrond. In heel specifieke gevallen bestaat wellicht de mogelijkheid dat gebruik van iRN/iColumbo door eindgebruikers nodig is ter vervulling van een wettelijke plicht. Realistischer is de mogelijkheid voor eindgebruikers dat de verwerking van persoonsgegevens noodzakelijk is voor de uitoefening van een publiekrechtelijke taak (artikel 8 e Wbp); het begrip 'noodzakelijk' moet – mede in het licht van art. 8 EVRM – echter strikt worden uitgelegd, en het is bij veel toepassingen door eindgebruikers de vraag of openbrononderzoek echt noodzakelijk is om hun publiekrechtelijke taak goed te kunnen uitoefenen. De ontwikkelaars en beheerders van iRN/iColumbo kunnen ook geen beroep doen op deze grondslag wanneer zij echte data gebruiken om de functionaliteit te testen of het systeem te beheren. In veel gevallen zullen eindgebruikers, en in alle gevallen zullen de ontwikkelaars en beheerders, daarom een beroep moeten doen op de verwerkingsgrond 8 onder f, de zogenoemde restgrond. Deze grond bepaalt dat gegevens verwerkt mogen worden als dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde, tenzij het recht van de betrokkene prevaleert. Aangezien het gaat om gegevens uit open bronnen, zal de privacyinbreuk voor betrokkenen vaak relatief gering zijn, zodat de belangenafweging vaak kan doorslaan in het voordeel van het belang van verantwoordelijken om openbrongegevens te verzamelen. Het gebruik van iRN/iColumbo moet dan wel een gerechtvaardigd belang dienen en het gebruik moet proportioneel zijn. Afhankelijk van de context en het gebruik van de verzamelde gegevens –

[11] Kamerstukken II, vergaderjaar 1997-1998, 25 892, nr. 3, p. 91.

bijvoorbeeld als er beslissingen worden genomen op basis van de data die voor betrokkenen negatieve gevolgen kunnen hebben – kan het belang van betrokkenen echter zwaarder gaan wegen en zal artikel 8 f Wbp niet als grondslag kunnen dienen. In die contexten zullen eindgebruikers dan alleen het systeem mogen gebruiken als het noodzakelijk is voor de uitoefening van hun publiekrechtelijke taak.

Naast het doel en de verwerkingsgrond, worden vervolgens eisen gesteld aan de **kwaliteit van de gegevens**. Zo moeten gegevens toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn met het oog op de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt (art. 11). Wat de **bewaartermijn** betreft geldt dat gegevens niet langer mogen worden bewaard in identificerende vorm dan nodig is voor het doel (art. 10). Vooral met betrekking tot gegevensverwerking in het kader van de ontwikkeling van iRN/iColumbo zal een korte bewaartermijn gelden. Gegevens mogen enkel bewaard worden tot het moment dat zij noodzakelijk zijn om de functionaliteit van iRN/iColumbo aan te tonen. Voor testdoeleinden bij ontwikkeling van systemen ligt het ook meer voor de hand om, als men met echte data uit open bronnen wil werken, persoonsgegevens die automatisch als zodanig herkend worden (door tools voor extractie van namen en adressen) te anonimiseren (of eventueel pseudonimiseren met beveiligde opslag van de pseudonimiseringscode, als er een gerechtvaardigd belang is om in aangewezen gevallen gegevens terug te herleiden tot individuen). (Over dit gebruik van omkeerbare pseudonimisering, zie par. 6.2.1 onder Minimaliseren en Verbergen.)

Een andere belangrijke verplichting is de in artikel 13 Wbp verankerde **beveiligingsplicht**:

> De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Het artikel geeft geen concrete handleiding welk niveau van beveiliging vereist is; dat hangt af van de risico's en de kosteneffectiviteit van mogelijke maatregelen. Aangezien bij iRN/iColumbo een grote hoeveelheid gegevens wordt verzameld en voor langere tijd opgeslagen, zullen hier wel hoge eisen worden gesteld aan de beveiliging, onder andere met het oog op risico's van hacken maar ook van mogelijk intern misbruik of nalatigheid die leidt tot datalekken. Indien een bewerker wordt ingeschakeld, moet de verantwoordelijke ervoor zorg dragen dat ook deze voldoende beveiligingsmaatregelen treft. Voor iRN/iColumbo zijn naast de beveiliging van gegevens ook mechanismen voor authenticatie en autorisatie van gebruikers van groot belang.

Naast de beveiligingsplicht geldt voor verantwoordelijken een **informatieplicht**, die is neergelegd in de artikelen 33 en 34 Wbp. De verantwoordelijke moet de betrokkene informeren over zijn identiteit en de doeleinden van de verwerking waarvoor de gegevens zijn bestemd; hij moet ook nadere informatie geven 'om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen', voor zover dat nodig is in verband met bijvoorbeeld het gebruik dat van de gegevens wordt gemaakt. Deze informatieplicht stelt dan de betrokkene in staat om zijn inzage- en correctierechten (art. 35 en 36) uit te oefenen. Overigens bepaalt art. 43 Wbp dat deze informatieplicht niet hoeft te worden toegepast als dat noodzakelijk is voor bepaalde publieke belangen. Voor de eindgebruikers die onder de Wbp vallen zal echter meestal niet de staatsveiligheid of een opsporingsbelang in het geding zijn; wel kan het belang spelen van toezicht op naleving van wetgeving ten behoeve van gewichtige economische en financiële belangen van de staat en andere openbare lichamen (art. 43 onder d j^{o} c). De vraag is echter of geheimhouding van de gegevensvergaring door bijvoorbeeld Belastingdienst Blauw of de AFM *noodzakelijk* is in het kader van hun toezichtstaak.

Als de uitzonderingsgrond van art. 43 niet opgaat, is het relevant te bepalen welk informatieregime van toepassing is. De Wbp maakt bij de informatieplicht onderscheid tussen verkrijging van gegevens bij de betrokkene zelf (art. 33) – dan moet de informatie vóór het moment van verkrijging worden verstrekt – en verkrijging op andere wijze (art. 34) – dan moet de informatie worden gegeven op moment van vastlegging (of als ze bestemd zijn voor verstrekking aan derden, op het moment van verstrekking, maar dat lijkt bij iRN/iColumbo niet het geval). De vraag is nu of het verzamelen van gegevens uit open bronnen kan worden gezien als het verkrijgen van gegevens 'bij de betrokkene'. In zeker opzicht is dat het geval, bij de gegevens die personen zelf op Internet hebben gezet, bijvoorbeeld op een webpagina, webforum of

socialenetwerkpagina. De betrokkene 'verstrekt' immers de gegevens zelf, zij het niet rechtstreeks en bewust aan de instanties die iRN/iColumbo gebruiken. Belangrijk is dan de voorzienbaarheid; de Memorie van Toelichting merkt voor art. 33 op:

> Hij zal dit doen [gegevens verstrekken] nadat hij – indien hij daarvan niet al op de hoogte is – is geïnformeerd over de identiteit van de houder en de doeleinden van de verwerking. Hij zal zich ook bewust moeten zijn van het feit dat hij gegevens verstrekt. De verstrekking moet zijn beoogd.[12]

De beoogde verstrekking hoeft niet altijd met volle bewustzijn te gebeuren; volgens de toelichting is bij cameratoezicht ook sprake van verkrijging van beelden bij de betrokkene (dus verstrekking van gegevens door de betrokkene) indien de camera maar duidelijk zichtbaar is en het doel van het cameratoezicht kenbaar is.[13] Aangezien de doelen van gegevensverzameling bij iRN/iColumbo heel divers zijn en ook niet kenbaar bij Internetgebruikers, concluderen wij dat in dit geval niet art. 33 maar art. 34 van toepassing is. Dat is relevant omdat de informatieplicht volgens art. 34 lid 4 niet geldt als het een onevenredige inspanning vergt om de betrokkenen te informeren. Deze uitzondering kan bij gebruik van iRN/iColumbo aan de orde zijn, omdat het niet doenlijk is om adresgegevens te achterhalen van alle individuen van wie persoonsgegevens op een of andere manier in het systeem worden verwerkt. In dat geval moet de verantwoordelijke wel de herkomst van de gegevens vastleggen (art. 34 lid 4); dat gebeurt bij iRN/iColumbo door het loggen van alle zoekacties en de terugspeelfunctie. Daartegen kan men inbrengen dat de informatieplicht wel uitgeoefend zou kunnen worden, enigszins vergelijkbaar met openbaar cameratoezicht, door het publiek algemeen te informeren over het gebruik van iRN/iColumbo (zie nader hfd. 7 over transparantie) en concreet bij elke zoekactie de identiteit kenbaar te maken door een herkenbaar IP-adres van de crawler. Met andere woorden: de informatieplicht van art. 34 Wbp kan impliceren dat het afschermen van de afkomst van gebruikers in iRN/iColumbo onrechtmatig is, omdat het de betrokkenen niet informeert wie bepaalde gegevens over hen vastlegt.

De artikelen 35 tot en met 42 van de Wbp bevatten verschillende **rechten van betrokkenen** met betrekking tot de persoonsgegevens die over hen verwerkt worden. Het gaat om een recht op inzage (art. 35),[14] verbetering, aanvulling, verwijdering, en afscherming (art. 36). Relevant om te vermelden is ook artikel 35 lid 4, dat bepaalt dat de verantwoordelijke op verzoek van de betrokkene mededelingen moet doen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens. In het kader van iRN/iColumbo betekent dit dat inzicht gegeven moet kunnen worden in de wijze waarop het systeem werkt. Voor zover bepaalde keuzes van omgang met persoonsgegevens ingegeven worden door de programmatuur/algoritmes die in iRN/iColumbo gebruikt worden, zoals automatische selectie en een bepaalde vorm van visualisatie van netwerkverbanden, dan moeten deze dus inzichtelijk gemaakt worden voor betrokkenen die hierom verzoeken. Op het inzagerecht van betrokkenen (en als uitvloeisel daarvan mogelijk ook het correctierecht) is overigens eveneens de uitzondering van art. 43 Wbp van toepassing (hierboven behandeld bij de informatieplicht); zoals daar aangegeven is het betwijfelbaar, of op zijn minst onduidelijk, of deze inroepbaar is voor eindgebruikers die onder de Wbp vallen.

In principe dient de verantwoordelijke in schriftelijke vorm aan verzoeken van de betrokkene op grond van artikel 35 en 36 te voldoen, tenzij een gewichtig belang van de betrokkene een andere vorm vereist (art. 37). Conform artikel 38 moet de verantwoordelijke ook derden aan wie hij eerder gegevens heeft verstrekt, in kennis stellen van de wijziging volgend op het verzoek van de betrokkene, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost. De artikelen 40 en 41 bieden betrokkenen een recht op verzet. Artikel 41 over direct marketing is hier niet relevant, maar artikel 40 wel. Het voorziet in een recht op verzet tegen verwerkingen gebaseerd op artikel 8 onder e of f Wbp. Zeker grond 8 onder f is een grond die vaak in zicht zal komen voor eindgebruik dat onder de Wbp valt (zie boven de alinea over 'legitieme verwerkingsgrond'). Dit recht van verzet houdt in dat wanneer een betrokkene verzet aantekent, de verantwoordelijke binnen vier weken beoordeelt of het verzet gerechtvaardigd is en als dat zo is, de verwerking van persoonsgegevens terstond beëindigt.

---

[12] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 156.
[13] Ibid.
[14] Op grond van artikel 39 Wbp mag een verantwoordelijke maximaal 5 euro vragen ter vergoeding om aan een verzoek op grond van artikel 35 Wbp te voldoen.

Hoofdstuk 4 van de Wbp geeft aan in welke gevallen de verantwoordelijke bovendien de plicht heeft om de verwerking van persoonsgegevens te **melden bij** de bevoegde nationale toezichthoudende autoriteit, in Nederland het College Bescherming Persoonsgegevens (**CBP**).[15] In de ontwikkelingsfase van iRN/iColumbo zullen de verwerkingen van persoonsgegevens die in dit kader plaatsvinden gemeld moeten worden bij het CBP. Het ligt op zich niet voor de hand dat het CBP een voorafgaand onderzoek uit zal willen voeren, aangezien de inbreuk op de persoonlijke levenssfeer in de ontwikkelingsfase gering is. Gegevens worden immers niet verzameld met als doel beslissingen over betrokkenen te nemen, maar puur om de functionaliteit te testen. Juist vanwege dit beperkte doel zal wel aan de overige randvoorwaarden uit de Wbp strikt de hand gehouden moeten worden, bijvoorbeeld zo min mogelijk persoonsgegevens verwerken en deze direct vernietigen zodra zij niet meer noodzakelijk zijn voor het testen. Ook eindgebruikers zullen het gebruik van het systeem moeten melden bij het CBP. Voor hen valt eerder te verwachten dat College dan een voorafgaand onderzoek zal doen. De Wbp is namelijk recentelijk op enkele punten gewijzigd.[16] Uit de combinatie van de artikelen 27 en 31 blijkt nu nog sterker dan voorheen dat verwerkingen in het kader van iRN/iColumbo die vallen binnen de werkingssfeer van de Wbp, alvorens daarmee te beginnen, gemeld moeten worden bij het College of bij de interne functionaris voor de gegevensbescherming. Bovendien moeten eindgebruikers rekening houden met een voorafgaand onderzoek door het College, wanneer de eindgebruiker 'voornemens is gegevens vast te leggen op grond van het gericht verzamelen van informatie door middel van eigen onderzoek zonder de betrokkene daarvan op de hoogte te stellen' (art. 31 lid 1 onder b). Naarmate eindgebruikers hun identiteit (IP-adres) meer afschermen en minder transparantie betrachten over het gebruik van het systeem in het algemeen, zal de kans groter zijn dat deze bepaling van toepassing is. Eindgebruikers moeten dan deze aard van de gegevensverwerking melden bij het College en mogen niet beginnen met gebruik van iRN/iColumbo totdat het onderzoek is afgerond dan wel het College bericht zendt dat het niet tot onderzoek zal overgaan (art. 32).

Een in *data mining*-contexten belangrijke bepaling is artikel 42 Wbp. Dit artikel beschermt betrokkenen tegen negatieve gevolgen van **geautomatiseerde beslissingen**. Het luidt, voor zover hier relevant:

> 1.Niemand kan worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van persoonsgegevens bestemd om een beeld te krijgen van bepaalde aspecten van zijn persoonlijkheid.
>
> 2.Het eerste lid is niet van toepassing, indien het daar bedoelde besluit: (...)
>
> b. zijn grondslag vindt in een wet waarin maatregelen zijn vastgelegd die strekken tot bescherming van het gerechtvaardigde belang van de betrokkene. (...)
>
> 4.In het geval, bedoeld in het tweede lid, deelt de verantwoordelijke de betrokkene de logica mee die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.

Wanneer bijvoorbeeld uit een trajectcontrolesysteem zou komen rollen dat persoon X op datum Y op het traject Z 50 kilometer per uur harder heeft gereden dan is toegestaan, mag niet automatisch op basis van dit systeemgegeven het rijbewijs van persoon X worden ingetrokken. Voor zover wij kunnen overzien, worden binnen iRN/iColumbo echter niet echt geheel geautomatiseerde beslissingen genomen over personen. Bij de interpretatie van verzamelde gegevens en de daarop volgende acties door eindgebruikers zullen naar wij aannemen altijd mensen betrokken zijn. Eén aspect van iColumbo is echter misschien wel relevant hier. De *crawl extender*-module in iRN/iColumbo biedt de mogelijkheid dat de crawler zelf het gevonden materiaal analyseert en op basis hiervan de crawlvragen uitbreidt, zonder verdere menselijke tussenkomst. Dat is geen besluit waaraan rechtsvervolgen zijn verbonden, maar het leidt wel tot verdere en nieuwe verwerkingen van persoonsgegevens, al dan niet van nieuwe betrokkenen, die zonder de *crawl extender* niet in beeld zouden zijn gekomen. Afhankelijk van de context en het gebruik dat vervolgens van die data wordt gemaakt, bestaat er wel een kans dat hierdoor een

[15] Hoofdstuk 4 van de Wbp betreft melding en voorafgaand onderzoek en hoofdstuk 9 betreffende toezicht gaat nader in op het CBP en de functionaris voor de gegevensverwerking.

[16] Wet van 26 januari 2012 tot wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen, *Staatsblad* 2012, 33.

betrokkene in aanmerkelijk mate getroffen wordt, bijvoorbeeld omdat hij in een bepaald licht komt te staan bij een overheidsinstantie die beslissingen over hem neemt (zoals belastingaanslagen of verklaringen omtrent het gedrag). Als dat zo is, dan legt art. 42 Wbp een verplichting op aan eindgebruikers om altijd een extra controle op het beeld dat ontstaan is na gebruik van de *crawl extender*, en in voorkomende gevallen de desbetreffende betrokkene te informeren over de manier waarop de *crawl extender* zoekvragen uitbreidt ('de logica die ten grondslag ligt aan' deze module), zodat hij de mogelijkheid heeft het hierdoor ontstane beeld recht te zetten.

Laag 2: Bijzondere persoonsgegevens

Bijzondere persoonsgegevens, ook wel gevoelige gegevens genoemd, zijn persoonlijke gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en betreffende het lidmaatschap van een vakvereniging. In het kader van iRN/iColmbo zou deze laag mogelijk het meest problematisch kunnen blijken. Net zoals bij het zoeken in open bronnen niet kan worden uitgesloten dat persoonsgegevens verwerkt worden, kan ook niet worden uitgesloten dat gevoelige gegevens verwerkt zullen worden. Immers, gevoelige gegevens zijn niet alleen vervat in tekst, maar bijvoorbeeld ook in foto- en videomateriaal. Uit een foto kan in veel gevallen ras of godsdienst (hoofddoek, keppel, kruisje) worden afgeleid en soms ook een gezondheidsaandoening. Het probleem in dezen is gelegen in het feit dat artikel 16 van de Wbp in beginsel de verwerking van gevoelige gegevens verbiedt. Het verwerkingsverbod geldt ook voor strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag (Art. 16 Wbp). Uiteraard bestaan er wel enkele uitzonderingen, die staan beschreven in de artikelen 17 -23 Wbp.

Eerst wordt in de artikelen 17 tot en met 22 per specifieke categorie bepaald welke uitzonderingen gelden met betrekking tot het verwerkingsverbod. Deze uitzonderingen zijn niet van toepassing op het zoeken in open bronnen. (Hooguit zouden strafrechtelijke opsporingsinstanties een beroep kunnen doen op artikel 22 als het gaat om het verzamelen uit open bronnen van strafrechtelijke persoonsgegevens, zoals over veroordelingen of gebiedsverboden, maar dat lost de problemen van de verwerking van andersoortige gevoelige gegevens, waaronder visueel materiaal, niet op.) Daarom zal moeten worden teruggevallen op de algemene uitzondering van artikel 23 Wbp: het verwerkingsverbod is niet van toepassing voor zover de verwerking geschiedt met uitdrukkelijke toestemming van de betrokkene; de gegevens door de betrokkene duidelijk openbaar zijn gemaakt; dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte; dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting; of dit noodzakelijk is met het oog op een zwaarwegend algemeen belang (waarbij dan passende waarborgen moeten worden getroffen en de verwerking hetzij op wettelijke grondslag hetzij met ontheffing van het CBP geschiedt; deze verwerkingen moeten op grond van lid 3 ook bij de Europese Commissie worden gemeld). Welke van deze uitzonderingen zou van toepassing kunnen zijn?

De redenering 'het staat in open bronnen dus de gegevens zijn door de betrokkene duidelijk openbaar gemaakt' zal slechts in enkele gevallen opgaan. In de Memorie van Toelichting bij de Wbp valt te lezen dat de openbaarheid van gegevens moet volgen uit 'gedrag van de betrokkene waaruit de intentie om openbaar te maken uitdrukkelijk blijkt'.[17] Het voorbeeld van een zichtbare handicap wordt gegeven om dit te verduidelijken: 'Dit gezondheidsgegeven is in veel gevallen voor een ieder zichtbaar, maar niet uit vrije wil aan de kant van de betrokkene. Dit gegeven mag derhalve niet op grond van onderdeel b worden verwerkt, tenzij de betrokkene zich als zodanig – bijvoorbeeld als belangenbehartiger voor gehandicapten – in de openbaarheid profileert.'[18] Alleen in die gevallen waarin zonder twijfel duidelijk is dat informatie door de betrokkene zelf in een open bron geplaatst is, met de intentie deze informatie kenbaar te maken aan het publiek, zal de verwerking op artikel 23 onder b gebaseerd kunnen worden. Het probleem met open bronnen is echter dat ook veel gegevens door derden worden gepubliceerd in plaats van door betrokkenen zelf, en het onderscheid tussen die twee is voor geautomatiseerde zoeksystemen niet of nauwelijks te maken. Het is voor de gebruiker van een systeem dat zoekt in open bronnen ook ondoenlijk om voor elk gegeven vast te stellen door wie het geplaatst is, laat staan met welke intentie. In het kader van het gebruik van iRN/iColumbo zal deze uitzondering dan ook zeker niet

[17] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 123.
[18] Ibid.

generiek uitkomst kunnen bieden. Voor eindgebruikers zal misschien onder omstandigheden wel een beroep gedaan kunnen worden op de grond 'uitoefening of de verdediging van een recht in rechte'. Bijvoorbeeld wanneer een verdachte claimt een whiplash opgelopen te hebben bij zijn aanhouding en daarvoor een civiele schadeclaim indient, zou de politie zijn openbare profielen op sociale netwerkpagina's kunnen raadplegen om de geloofwaardigheid van de claim te toetsen; als daar dan foto's staan van een headbangende verdachte op een *heavy metal*-feestje, kan de politie deze informatie gebruiken ter verdediging van een recht in rechte. Vaak zal zo'n situatie zich echter niet voordoen.

Als uiterste restgrond geldt dat de uitzondering dat verwerking van gevoelige gegevens geoorloofd is voor zover dit 'noodzakelijk is met het oog op een zwaarwegend algemeen belang'. De reden waarom dit de uiterste restgrond is, is gelegen in het feit dat deze enkel ingeroepen kan worden indien passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het CBP ontheffing heeft verleend. In dit kader kan het College bij de verlening van ontheffing beperkingen en voorschriften opleggen.

Art. 16 Wbp heeft implicaties voor zowel de systeemontwikkelaars als de eindgebruikers van iRN/iColumbo. Voor de ontwikkelaars geldt dat het testen van functionaliteiten en de werking van het iColumbo-raamwerk of afzonderlijke modules niet onder een uitzonderingsgrond zal vallen. (Wellicht kunnen op deelonderwerpen onderzoekers zich nog beroepen op art. 23 lid 2, wanneer het verwerken van gevoelige gegevens wanneer het wetenschappelijk onderzoek een algemeen belang dient en het noodzakelijk is om daarvoor gevoelige gegevens te verwerken; meestal zal dit laatste echter niet noodzakelijk zijn omdat er minder ingrijpende alternatieven voorhanden zijn.) De ontwikkelaars van iRN/iColumbo zullen binnen de kaders van ontwikkeling daarom alleen mogen werken hetzij met fictieve data hetzij met echte data uit open bronnen waarbij geen enkel visueel materiaal wordt gebruikt. Als het voor testen van bepaalde modules onvermijdelijk is om visueel materiaal uit bestaande open bronnen te gebruiken, zal ontheffing gevraagd moeten worden aan het CBP en zullen passende waarborgmaatregelen moeten worden getroffen (zoals het geautomatiseerd onherkenbaar maken van gezichten in foto's of video's).

Eindgebruikers die onder de Wbp vallen kunnen iets eerder dan de systeemontwikkelaars een beroep doen op art. 23, maar ook voor hen zijn de eisen restrictief: het moet gaan om een *zwaarwegend* algemeen belang en de verwerking van gevoelige gegevens moet daarvoor *noodzakelijk* zijn. Voor de meer algemene, verkennende zoekacties van iRN/iColumbo zal dit nooit gelden; alleen voor bepaalde concrete en ernstige zaken waarin beeldmateriaal een belangrijke rol zal moeten spelen om de zaak op te lossen, zal het verwerken van gevoelige gegevens gelegitimeerd kunnen worden. Zolang er geen expliciete wettelijke bepaling is die zegt dat de eindgebruiker voor dit doel gevoelige gegevens mag verwerken, zal de eindgebruiker daarbij ontheffing moeten vragen aan het CBP, en eveneens waarborgmaatregelen moeten nemen om de privacyinbreuk zo klein mogelijk te houden.

Laag 3: Doorgifte naar derde landen

De derde laag van het gegevensbeschermingsregime betreft de doorgifte van persoonsgegevens naar derde landen, ofwel landen buiten de EU en de EER. Uitgaande van de situatie dat iRN/iColumbo gebruikt wordt door eindgebruikers die gevestigd zijn in Nederland en die de verzamelde data ook opslaan op Nederlands grondgebied, zal er geen sprake zijn van doorgifte naar derde landen. Er wordt wel over de landsgrenzen heen data verzameld, maar hierbij worden de data juist vanuit andere landen naar Nederland geïmporteerd. Indien eindgebruikers ervoor zouden kiezen de met iRN/iColumbo verzamelde gegevens op te slaan op buitenlands grondgebied, bijvoorbeeld met gebruikmaking van clouddiensten waarbij gegevens op wisselende servers op wisselende locaties staan, wordt de laag betreffende doorgifte van persoonsgegevens naar derde landen wel zeer relevant. Gezien de complexiteit die dit met zich brengt en de gevoeligheid van de (combinaties van) gegevens die met iRN/iColumbo verzameld kunnen worden en de vergaande consequenties die het gebruik van met iRN/iColumbo gegenereerde gegevens kan hebben voor betrokkenen, wordt aanbevolen gegevens lokaal, dat wil zeggen binnen het Nederlandse territoir, op te slaan.

2.3.4. Privacyaspecten van het loggen van iRN/iColumbo-gebruik

Vanuit een oogpunt van transparantie en controleerbaarheid van het gebruik dat gemaakt wordt van iRN/iColumbo (zie hfd. 7), is het een pluspunt dat alles wat er met het systeem gedaan wordt, gelogd wordt. Dit houdt in dat bij zoekacties geregistreerd wordt wie wanneer op basis van

welke zoekvraag wat zoekt Ook voor het kunnen gebruiken van de met iRN/iColumbo gegenereerde gegevens in de bewijsvoering, bijvoorbeeld in strafzaken, is het extensief loggen van het gebruik van iRN/iColumbo wenselijk. Het extensief loggen van het gebruik van het systeem heeft echter ook een nadeel, aangezien het persoonsgegevens van individuele gebruikers genereert (waarbij we op basis van de interviews aannemen dat de identiteit van de individuele gebruikers wordt meegelogd). Dit is een vorm van verwerking van persoonsgegevens, die dan ook weer aan wettelijke verplichtingen gebonden is.

Hoewel het loggen een intrinsiek onderdeel van het systeem iRN/iColumbo vormt, kan niet in zijn algemeenheid gesteld worden dat dit loggen geschiedt ten behoeve van de politietaak. Ook bij de ontwikkeling van iRN/iColumbo worden persoonsgegevens verwerkt, en bovendien is er ook het nodige eindgebruik voorzien dat niet onder de politietaak valt, bijvoorbeeld bij Belastingdienst Blauw. Door de ontwikkelaars van het systeem en door de eindgebruikers zal in de doelomschrijving dan ook meegenomen moeten worden dat in het kader van deze verwerking ook persoonsgegevens (namelijk loggegevens) worden verwerkt van werknemers die het systeem gebruiken. Belangrijk in dit verband is dat het systeem niet meer logt dan enkel gegevens die betrekking hebben op de persoon die op dat moment het systeem gebruikt. Op deze wijze kunnen de verwerkingen in het kader van loggen namelijk via contractuele weg worden geregeld. Dit heeft voordelen boven andere grondslagen uit art. 8 Wbp, zoals toestemming (die ingetrokken zou kunnen worden) of de restgrond onder f (waarbij bijvoorbeeld het recht op verzet kan gelden). Wanneer het loggen onlosmakelijk verbonden is aan het gebruik van iRN/iColumbo, dan is het verwerken van persoonsgegevens in dit kader te kwalificeren als een noodzakelijke verwerking in het kader van de uitvoering van de overeenkomst (tussen eindgebruiker en beheerder) om iRN/iColumbo te kunnen gebruiken. De werknemer bij de eindgebruiker zal wel duidelijk geïnformeerd moeten worden over welke gegevens precies verwerkt worden, wat precies het doel is van de verwerking, hoe lang deze gegevens verwerkt zullen worden, enzovoorts. Dit omdat in het kader van het loggingproces de regels van de Wbp (dan wel van de Wet politiegegevens bij opsporingsdiensten) onverkort van toepassing zijn. Wanneer het loggen van gegevens over individuele gebruikers niet onlosmakelijk met het systeem verbonden is, bijvoorbeeld als die een functionaliteit zou zijn die aan- of uitgeschakeld kan worden (wat vanuit het oogpunt van privacybescherming van werknemers wellicht de voorkeur verdient), dan zou het loggen van individuele werknemers ook geregeld kunnen worden via het arbeidscontract; zo'n bepaling moet dan wel redelijk zijn om binnen de contractsvrijheid van werknemers in een asymmetrische relatie met hun werkgever te passen; dat kan als dergelijk loggen passend is binnen de context van de normale taakuitoefening, wat per eindgebruiker kan verschillen). Voor opsporingsdiensten waarbij gebruik van iRN/iColumbo bruikbaar moet zijn als bewijs in de rechtszaal, lijkt het loggen van individueel gebruik nodig in verband met de controleerbaarheid van het bewijs; in dat geval is het loggen te rechtvaardigen op de grond van noodzaak ter uitvoering van een publieke taak (artikel 8 onder e).

Tot slot moet hier ook worden gewezen op artikel 27 lid 1 onder l van de Wet op de ondernemingsraden. Dit artikel luidt:

> 1. De ondernemer behoeft de instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van: (…)
> l. een regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen.

Aangezien de logging van iRN/iColumbo impliceert dat de aanwezigheid en het gedrag van gebruikers van het systeem (en wellicht ook hun prestaties) gecontroleerd kunnen worden, zal de ondernemingsraad met iRN/iColumbo, met name in relatie tot de daarin geïntegreerde logfunctie, in moeten stemmen.

2.4. Internationale aspecten

Bij gebruik van iRN/iColumbo worden over de landsgrenzen heen data verzameld. Het is mogelijk dat dit verzamelen in strijd is met de wetgeving van het land van waaruit die gegevens worden aangeboden. Binnen het kader van deze studie is het niet mogelijk om de privacy- en persoonsgegevenswetgeving van alle landen op dit aspect te analyseren. We volstaan hier met de constatering dat over het algemeen wordt gesteld dat in de Europese Unie een hoog niveau van bescherming van persoonsgegevens bestaat, zodat mag worden aangenomen dat het

onwaarschijnlijk is dat ontwikkelaars of gebruikers van iRN/iColumbo inbreuk maken op de privacy- of persoonsgegevenswetgeving van andere landen zolang zij voldoen aan de eisen van de Wbp.

2.5. Korte blik op de toekomst

De Dataprotectierichtlijn dateert uit 1995 en kent bovendien nogal wat verschillen in implementatie in de verschillende lidstaten. Om de bescherming van persoonsgegevens bij de tijd te brengen met een geharmoniseerd niveau van bescherming, heeft de Europese Commissie op 25 januari 2012 voorstellen uitgevaardigd om Richtlijn 95/46/EG te vervangen door een Verordening.[19] Het verschil met een Richtlijn is dat een Verordening niet omgezet hoeft te worden in nationaal recht, maar direct doorwerkt in de nationale rechtsordes. Hiermee worden implementatieverschillen voorkomen. Naast een voorstel voor een algemene Dataprotectieverordening wordt tevens voorgesteld het Kaderbesluit 2008/977/JBZ (persoonsgegevens in de politiële en justitiële sector)[20] te vervangen door een Richtlijn voor gegevensbescherming in de strafrechtelijke context.[21] Aangezien zowel het Europees Parlement als de Europese Raad in eerste en in tweede lezing nog met wijzigingsvoorstellen kunnen komen, is het verre van zeker dat de huidige tekstvoorstellen gehandhaafd zullen blijven. Ook zal het nog minstens enkele jaren duren voordat het gewijzigde regime in werking zal treden (na goedkeuring treedt de wet na twee jaar in werking). Gezien de onzekere toekomst is het niet relevant om te speculeren over wijzigingen in het regime die de ontwikkeling van iRN/iColumbo zouden kunnen raken. We volstaan hier met het noemen van de in het algemeen meest substantiële wijzigingen. Meldingsplichten bij de toezichthoudende instanties verdwijnen maar worden vervangen door een verplichting om zeer uitgebreid interne documentatie bij te houden over gegevensverwerking. Een recht om vergeten te worden wordt geïntroduceerd, alsmede de concepten van gegevensbescherming 'by design' en 'by default'. De nationale toezichthoudende instanties krijgen meer bevoegdheden om te handhaven en bovendien wordt de mogelijkheid gecreëerd hoge administratieve boetes op te leggen bij overtreding van regels betreffende verwerking van persoonsgegevens.

Verder is van belang een consultatie die tot eind februari 2012 liep betreffende conceptwetsvoorstel ter wijziging van de Wbp in verband met een algemene meldplicht datalekken.[22] De algemene meldplicht datalekken moet gelden voor zowel publieke als private partijen. De meldplicht is zeer verglijkbaar met de eerder voorgestelde meldplicht uit de Telecommunicatiewet. Datalekken zullen nu aan het CBP gemeld moeten worden, waarbij een sanctie van 200.000 euro kan worden opgelegd. Het CBP heeft over de wijzigingswet geadviseerd om de meldplicht alleen in het wetsvoorstel op te nemen als met twaalf punten rekening is gehouden.[23] Hierbij gaat het onder andere om een betere afstemming met de meldplicht zoals neergelegd in de Europese ontwerp-Verordening, het nader specificeren van termijnen, vormvereisten en boetebepalingen.

2.6. Conclusie

Uit deze paragraaf valt te concluderen dat de Wbp van toepassing is op de ontwikkelaars van iRN/iColumbo voor zover zij in het kader van de ontwikkeling van deze systemen

[19] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.1.2012, COM(2012) 11 final, te raadplegen op: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[20] Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, PubEG Nr. L 350 van 30/12/2008, p. 0060 - 0071

[21] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.1.2012, COM(2012) 10 final, te raadplegen op: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf.

[22] Wijzigingswet en consultatie beschikbaar via: http://internetconsultatie.nl/camerabeelden.

[23] Advies wetsvoorstel gebruik camerabeelden en meldplicht datalekken, 15 maart 2012, z2011-00970. Advies CBP is beschikbaar via: http://www.cbpweb.nl/downloads_adv/z2011-00970.pdf.

persoonsgegevens uit open bronnen verwerken. Hetzelfde geldt voor eindgebruikers, tenzij zij persoonsgegevens verwerken in het kader van de politietaak (zoals door de politie of de FIOD-ECD ter opsporing van strafbare feiten) of van een andere in de Wbp genoemde uitzondering. Op verwerking in het kader van de politietaak is het regime van de Wet politiegegevens van toepassing (zie par. 4.1.5). Hierbij moet wel worden opgemerkt dat uit de interviews met de Belastingdienst blijkt dat de douane, in nauwe samenwerking met of onder de vlag van de FIOD-ECD, ook betrokken kan zijn bij opsporing. Het is daarom van groot belang dat het gebruik van iRN/iColumbo juridisch en organisatorisch goed wordt ingekaderd zodat altijd helder is voor welke taak organisatieonderdelen het systeem gebruiken. Alleen dan kunnen gebruikers weten of ze onder het Wbp-regime vallen of onder het regime van de Wet politiegegevens.

De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens bepaalt is verantwoordelijk voor de verwerking van die persoonsgegevens en moet ervoor zorg dragen dat de relevante regelgeving wordt nageleefd. De Wbp gaat hierbij uit van diegene die daadwerkelijk in de praktijk doel en middelen bepaalt, en niet om diegene die mogelijk op papier is aangewezen als verantwoordelijke. Op de verantwoordelijke rust tevens de plicht om te zorgen dat eventuele bewerkers zich aan de geldende wet- en regelgeving houden. Een belangrijke vraag die in het kader van de ontwikkeling van iRN/iColumbo beantwoord moet worden betreft dan ook: wie is aan te merken als de verantwoordelijke met betrekking tot de verwerking van persoonsgegevens die plaatsvindt in het kader van iRN/iColumbo? Vanuit het perspectief van artikel 8 EVRM moet bovendien gespecificeerd worden op basis van welke wettelijke grondslag eventuele inbreuken op de privacy die het gebruik van iRN/iColumbo met zich brengt gestoeld kunnen worden. Ook moet de noodzaak van een dergelijk systeem in onze democratische samenleving onderbouwd worden en moet aandacht besteed worden aan de proportionaliteit en de subsidiariteit van de systemen. Hierbij is het van belang dat al in de fase van ontwikkeling aandacht wordt besteed aan vragen als: kan middels de techniek vormgegeven worden aan/tegemoet gekomen worden aan concepten als dataminimalisatie (niet meer data verwerken dan noodzakelijk is voor het doel), transparantie (hoe kan het systeem betrokkenen informeren, hoe kan de wijze waarop gegevens worden verwerkt zo inzichtelijk mogelijk worden gemaakt) en verantwoording (hoe kan een rechtmatige gang van zaken aangetoond worden, bijvoorbeeld het loggen van de informatie).

3. Auteursrecht en databankenrecht

3.1. Inleiding

iRN en iColumbo maken gebruik van gegevens uit openbare bronnen. Openbare bronnen zijn die bronnen waartoe een ieder rechtmatig toegang heeft; er bestaat verschil van mening of ook bronnen waarvoor iedereen toegang kan krijgen tegen betaling of na registratie onder 'open bronnen' vallen. Ongeacht de precieze reikwijdte, het feit dat informatie beschikbaar is in openbare bronnen betekent niet dat er geen intellectuele eigendomsrechten op de gegevens in die bronnen kunnen rusten. Indien intellectuele eigendomsrechten rusten op gegevens in openbare bronnen, dan moet het kopiëren, bewerken en verspreiden van die gegevens de daarop rustende rechten respecteren. Er zijn velerlei intellectuele eigendomsrechten, zoals octrooien, merkrechten, auteursrechten en naburige rechten. In dit rapport kijken we alleen naar de voor iRN en IColumbo belangrijkste intellectuele eigendomsrechten, te weten het auteursrecht en het databankenrecht.

3.2. Auteurswet

In deze paragraaf wordt eerst bezien wat het auteursrecht beschermt. Vervolgens wordt bezien welke ruimte het auteursrecht laat voor omgang met werken in het kader van iRN en iColumbo.

3.2.1. Wat is beschermd?

Het auteursrecht beschermt werken van letterkunde, wetenschap en kunst. Een werk wordt door het auteursrecht beschermd als het tot uitdrukking is gebracht en het origineel is in die zin dat het een eigen intellectuele schepping van de auteur is.[24] In de praktijk is dat een niet zo heel erg hoge drempel. Een auteursrecht komt 'automatisch' tot stand bij het voltooien van een werk. Het hoeft dus niet aangevraagd of geregistreerd te worden. Veel van wat op Internet staat is dan ook potentieel beschermd onder het auteursrecht. Dit roept de vraag op of dan ook 'alles' wat op Internet staat auteursrechtelijk beschermd is – tweets, blogs, *user generated content*? Op basis van de huidige jurisprudentie wordt veel informatie op het Internet bestreken door het auteursrecht. De belangrijkste rechterlijke uitspraken geven het volgende beeld te zien.

De afzonderlijke woorden in een tekst genieten geen bescherming, maar een combinatie van woorden mogelijk weer wel:[25]

> Met betrekking tot de beschermde bestanddelen van dergelijke werken zij opgemerkt dat deze bestaan uit woorden die, afzonderlijk beschouwd, als dusdanig geen intellectuele schepping van de auteur die ze gebruikt, vormen. Enkel via de keuze, de schikking en de combinatie van deze woorden op een oorspronkelijke wijze kan de auteur uitdrukking aan zijn creatieve geest geven en tot een resultaat komen dat een intellectuele schepping vormt.

Uit het Infopaq-arrest blijkt dat bescherming ook kan bestaan voor korte werken. Het bedrijf Infopaq haalde extracten van 11 woorden lengte uit persartikelen. Was er sprake van een gedeeltelijke reproductie in de zin van art. 2 Auteursrechtrichtlijn (2001/29/EC)? Het EU Hof van Justitie oordeelde als volgt:[26]

> Gelet op de eis van een ruime uitlegging van de omvang van de door artikel 2 van richtlijn 2001/29 verleende bescherming kan niet worden uitgesloten dat bepaalde afzonderlijke zinnen, of zelfs zinsneden van de betrokken tekst, de oorspronkelijkheid van een publicatie zoals een persartikel aan de lezer kunnen overdragen via het overbrengen van een bestanddeel dat in se de uitdrukking vormt van de eigen intellectuele schepping van de auteur van dit artikel. Dergelijke zinnen of zinsneden kunnen dus in aanmerking komen voor de op grond van artikel 2, sub a, van deze richtlijn geboden bescherming.

[24] EUHvJ 16 juli 2009, C-5/08 Infopaq, r.o. 37, bevestigd in EUHvJ 4 oktober 2011, C-403/08 en C-429/08 (Premier League).
[25] EUHvJ 16 juli 2009, C-5/08 Infopaq, r.o. 45.
[26] EUHvJ 16 juli 2009, C-5/08 Infopaq, r.o. 47-48.

> Gelet op deze overwegingen kan de weergave van een fragment uit een beschermd werk dat – zoals in het hoofdgeding – bestaat uit elf opeenvolgende woorden ervan, een gedeeltelijke reproductie in de zin van artikel 2 van richtlijn 2001/29 vormen indien – hetgeen de verwijzende rechter dient na te gaan – een dergelijk fragment een bestanddeel van het werk omvat dat als dusdanig uitdrukking geeft aan de eigen intellectuele schepping van de auteur.

Het is niet relevant of iemand de intentie heeft een werk te scheppen. Dit blijkt uit het arrest van de Hoge Raad in de Endstra-zaak:[27]

> Het gaat hierbij evenwel om een kenmerk dat uit het voortbrengsel zelf is te kennen. Daarom mag niet de eis worden gesteld dat de maker bewust een werk heeft willen scheppen en bewust creatieve keuzes heeft gemaakt, welke eis betrokkenen bovendien voor onoverkomelijke bewijsproblemen kan stellen. Om dezelfde reden kan niet worden geëist dat de maker bewust voor de vorm heeft gekozen die het werk heeft gekregen. Het in 4.5.1 overwogene brengt voorts mee dat een schepping, om een werk in auteursrechtelijke zin te kunnen zijn, niet het karakter van een coherente creatie behoeft te hebben.

Deze overwegingen wijzen erop dat veel van wat op Internet staat auteursrechtelijk beschermd zal zijn. (De vraag is daarbij wel of het wel zo gelukkig als 'overal' auteursrechtelijke bescherming voor bestaat; daarop gaan we nader in in par. 3.5.)

Uit de vraag of een werk voor bescherming in aanmerking komt, volgt de vraag hoe de rechthebbende zijn rechten uitoefent en welke ruimte er bestaat voor derden om van beschermd materiaal gebruik te maken. Daarover gaat de volgende paragraaf.

3.2.2. Ruimte voor omgang met werken

De rechthebbende op een werk heeft een aantal economische exclusieve rechten:

- Het **reproductierecht**, dat ook reproducties in het digitale domein omvat, zoals downloads. Een kopie van digitale gegevens van voorbijgaande aard (zoals een kopie in RAM-geheugen) is onder omstandigheden (art. 13a Aw) geen reproductie; aangezien iRN/iColumbo gevonden gegevens ook buiten het werkgeheugen opslaat, zal er steeds sprake zijn van reproducties.
- Het **openbaarmakingsrecht**. In wezen is 'openbaarmaking' een koepelbegrip. De verschillende vormen van openbaarmaking kunnen onderscheiden worden in materiële en immateriële vormen van openbaarmaking. Onder het eerste is het distributierecht te begrijpen, dat wil zeggen het verspreiden van exemplaren (dragers met daarin vastgelegd een werk) of het aanbod daartoe. Bij immateriële openbaarmaking wordt doorgaans onderscheid gemaakt tussen openbaarmaking ter plaatse en op afstand en tussen openbaarmaking waarbij het gehele publiek tegelijkertijd het werk consumeert en vormen waarbij leden van het publiek op een zelf gekozen tijdstip het werk consumeren. Ter illustratie:
    - op- of uitvoering en voordracht (ter plaatse en gehele publiek tegelijkertijd);
    - radio- of TV-uitzending (op afstand en gehele publiek tegelijkertijd);
    - beschikbaarstelling op een intern netwerk voor raadpleging binnen een gebouw, zoals een bibliotheek (ter plaatse en niet tegelijkertijd);
    - beschikbaarstelling op een Internetpagina (op afstand en niet tegelijkertijd).
- Het recht om een **vertaling**, **bewerking** of muziekschikking te maken.

Iedere handeling met betrekking tot een werk die onder een van de exclusieve rechten valt, is in beginsel onderworpen aan toestemming van de rechthebbende. Andere handelingen, zoals het lezen van een werk, zijn vrij.

De rechthebbende kan derden toestemming verlenen om relevante handelingen (reproduceren, openbaar maken, bewerken) te verrichten. Die toestemming wordt doorgaans verleend in de vorm van een licentie. Die licentie kan een algemeen en gratis karakter hebben, bijvoorbeeld de Creative Commons-licentie of verschillende vormen van *open source*-licenties voor software. Een licentie kan ook tot een specifieke licentienemer gericht zijn en verbintenissen voor de licentienemer inhouden, zoals betaling van een royalty. Een licentie kan ook een impliciet karakter hebben. Een rechthebbende die een werk op het openbare deel van het Internet ter download beschikbaar stelt, verleent impliciet een licentie de reproductie te verrichten die noodzakelijkerwijze het gevolg is van downloaden.

[27] HR 30 mei 2008, LJN: BC2153, IER 2008, 58 m.nt. JMBS, JOL 2008, 434, NJ 2008, 556 m.nt. E.J. Dommering en RvdW 2008, 567, par. 4.5.2.

Voor een aantal specifieke situaties kent het auteursrecht uitzonderingen op de exclusieve rechten. Voorbeelden daarvan zijn de privékopie, het citaat en het overnemen door de pers. Indien zich zo'n uitzonderingsituatie voordoet mogen derden relevante handelingen verrichten zonder licentie van de rechthebbende.

De Auteurswet kent in art. 22 een voor iRN/iColumbo relevante uitzondering op de exclusieve rechten van de auteur:

> 1. In het belang van de openbare veiligheid alsmede ter opsporing van strafbare feiten mogen afbeeldingen van welke aard ook door of vanwege de justitie worden verveelvoudigd of openbaar gemaakt.
>
> 2. Als inbreuk op het auteursrecht op een werk van letterkunde, wetenschap of kunst wordt niet beschouwd het overnemen ervan ten behoeve van de openbare veiligheid of om het goede verloop van een bestuurlijke, parlementaire of gerechtelijke procedure of de berichtgeving daarover te waarborgen.

Het tweede lid – dat ter implementatie van art. 5(3)(e) Richtlijn 2001/29/EG[28] is ingevoegd – is daarbij het interessantste omdat het voor alle werken geldt en niet slechts voor afbeeldingen. Volgens Spoor/Verkade/Visser mag het woord 'overnemen' in het tweede lid ruim worden geïnterpreteerd en omvat het alle vormen van verveelvoudigen en openbaar maken (de richtlijn spreekt van 'gebruik').[29] Of 'overnemen' zich ook uitstrekt over vertalen en bewerken is echter niet duidelijk. De hamvraag bij de bepaling van het tweede lid is uiteraard wanneer er sprake is van overnemen ter waarborging van de openbare veiligheid of het goede verloop van de genoemde procedures. Het is immers niet aan te nemen dat bestuurders, parlementsleden, rechters, advocaten en AIVD-medewerkers met een beroep op deze bepaling gratis en onbeperkt elk beschermd werk mogen kopiëren en openbaar maken. Uit de ons bekende rechtspraak is daarover echter niet veel af te leiden.

In de parlementaire geschiedenis van het wetsvoorstel waarbij het tweede lid is ingevoegd, is de bepaling nauwelijks besproken. In de Memorie van Toelichting wordt het volgende gemeld:[30]

> Met de in deze bepaling geboden mogelijkheid is niet alleen een algemeen (preventie-, opsporings- en vervolgings-) belang betrokken, maar wordt tevens het bestuurlijke, parlementaire en gerechtelijke proces gediend. Deze begrippen zullen nadere invulling door de rechter behoeven.

De eerste geciteerde zin blinkt niet uit in duidelijkheid. Niettemin lijkt het expliciet naast elkaar noemen van preventie, opsporing en vervolging te duiden op een ruim toepassingsbereik. Met enige goede wil is daar allicht ook digitale surveillance onder te begrijpen. Surveilleren kan immers preventie- en vervolgingsdoeleinden dienen. Echter, surveilleren kan ook andere dan de hier genoemde doelen dienen, zoals controle van bestuurswetgeving. Enige onduidelijkheid over de precieze reikwijdte van de bepaling blijft daarmee bestaan.

Ook over de term 'gerechtelijke of bestuurlijke procedure' bestaat geen duidelijkheid. Zij worden in de Auteurswet ook nog genoemd in art. 16b lid 4 en 16c lid 7 (beide over de uitzondering voor privékopieën). Ons is echter geen rechtspraak bekend die de betekenis van deze termen nader verduidelijkt. Wellicht kan men ervan uitgaan dat onder een bestuurlijke procedure alles is te verstaan wat een bestuursorgaan in de uitoefening van haar publiekrechtelijke taak verricht. Dat is een ruime omschrijving en omvat ook die werkzaamheden die verricht worden als nog geen bestuurlijke beschikking in zicht is. Maar mogelijk is de reikwijdte van de exceptie beperkter en alleen beschikbaar voor bestuursorganen in het kader van concrete beschikkingen en aanhangige geschilprocedures. In het laatste geval zou het gebruik van iRN/iColumbo zich dan moeten beperken – tenzij men toestemming van auteursrechthebbenden heeft verworven – tot het gebruik van het systeem in concrete bestuurlijke of rechtszaken, en zou het gebruik van het systeem voor de algemene uitoefening van de taak (zoals algemene verkenningen door Belastingdienst Blauw of de Autoriteit Financiële Markten) inbreuk maken op de auteursrechten van rechthebbenden.

De regering meldt – zoals we hierboven hebben gezien – dat de in het tweede lid van art. 22 Aw genoemde begrippen 'nadere invulling door de rechter' behoeven. Helaas is er tien jaar na dato weinig rechtspraak beschikbaar die de benodigde duidelijkheid kan verschaffen. Het EU Hof

[28] Richtlijn 2001/29/EG van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij, *PbEG* L 167 van 22.6.2001, p. 10–19.
[29] Spoor, Verkade & Visser 2005, p. 297.
[30] *Kamerstukken II* 2001/02, 28 482, nr. 3, p. 54.

van Justitie bepaalde dat een uitgever zich niet zelfstandig op de openbare veiligheid (als genoemd in de bepaling) kan beroepen.[31] Het ging in deze zaak om een fotografe die zich verzette tegen het gebruik van een door haar gemaakte kinderfoto van Natascha Kampusch in de pers. De desbetreffende uitgever beriep zich op de exceptie voor openbare veiligheid.

> Een dergelijke uitgever mag dus niet op eigen initiatief een door een auteursrecht beschermd werk gebruiken met een beroep op een doel van openbare veiligheid.
>
> Aangezien de pers in een democratische samenleving en een rechtsstaat tot taak heeft, zonder andere dan de strikt noodzakelijke beperkingen het publiek te informeren, kan niet worden uitgesloten dat een persuitgever in individuele gevallen tot de bereiking van een doel van openbare veiligheid kan bijdragen door een foto van een gezochte persoon te publiceren. Wel moet het initiatief daartoe worden genomen in het kader van een beslissing of actie van de bevoegde nationale autoriteiten die ertoe strekt de openbare veiligheid te verzekeren, en in overleg en in coördinatie met die autoriteiten, om te voorkomen dat de uitvoering van de door deze laatste getroffen maatregelen wordt belemmerd. Een concrete, actuele en uitdrukkelijke oproep van de met de veiligheid belaste autoriteiten om ten behoeve van een onderzoek een foto te publiceren is echter niet noodzakelijk.

Dit arrest bevestigt dat de exceptie niet slechts beperkt is tot reproducties maar zich ook uitstrekt tot openbaarmakingen. Over de betekenis van openbare veiligheid leert het arrest ons niet veel anders dan dat de opsporing van vermiste personen kennelijk in het belang van de openbare veiligheid is.

3.2.3. Auteursrechten op tools

De voor iRN en iColumbo meest pregnante auteursrechtproblemen doen zich voor bij auteursrechten op materiaal uit open bronnen. De computerprogramma's die in het kader van iRN en iColumbo worden ontwikkeld kunnen en zullen in de praktijk echter ook beschermd zijn door auteursrechten. Dat levert in het algemeen geen bijzondere problemen op. Niettemin verdient een aspect aandacht. Soms zijn tools een doorontwikkeling van een computerprogramma dat verkregen is onder een *free* of *open source*-licentie, zoals de General Public License (hierna: GPL). Die licenties bevatten vaak een zogenaamde *copyleft*-bepaling, zoals art. 5 & 6 GPL v3. Op basis van die bepalingen moet de programmeur van een modificatie op een programma dat onder een GPL v3 licentie is verkregen, wanneer hij het gemodificeerde programma publiek beschikbaar maakt, dat ook doen onder de GPL v3. Dat impliceert dat hij dan ook de broncode van de modificatie beschikbaar moet maken. Het publiek beschikbaar komen van de broncode maakt het echter voor een ieder gemakkelijk de precieze werking van het programma te achterhalen, wat nadelige gevolgen kan hebben bij de inzet van het programma voor iRN/iColumbo ondersteunde doeleinden. Het wordt dan immers mogelijk te anticiperen op wat de programmatuur kan en vooral ook niet kan. In dit opzicht is er een spanning tussen de wens bij de iRN/iColumbo-beheerders om transparant en controleerbaar te zijn en de wens om effectief te kunnen opereren.

Indien in een concreet geval de afweging tussen transparantie en effectiviteit in het voordeel van het laatste uitvalt, dan is het van belang om te bezien welke ruimte de GPL v3 laat om te modificeren en te delen zonder daarbij de broncode te moeten vrijgeven. De GPL v3 biedt ruimte als een programma verspreid wordt op zodanige wijze dat de ontvanger van het programma zelf geen additionele kopieën van het programma kan maken of ontvangen.[32] In dat geval is verspreiding zonder nadere voorwaarden toegestaan en dat impliceert dan ook dat niet de voorwaarde geldt dat aan degene aan wie het programma beschikbaar gesteld wordt de GPL v3 wordt opgelegd. Dat biedt perspectief voor iColumbo. Als iColumbo beschikbaar wordt gesteld aan gebruikers op een dusdanige manier dat de gebruiker zelf geen kopieën van het programma kan maken, dan is verspreiding van eventuele in iColumbo vervatte componenten die onder een GPL v3-licentie zijn verkregen geen probleem. Mogelijk dat iColumbo-componenten nu reeds op die manier verspreid worden, al was het maar om enige controle te houden over de verspreiding ervan in executable vorm. Allicht dat andere *open source*- of *free* licenties dan de GPL dergelijke ruimte ook bieden, maar dat blijft iets dat in voorkomende gevallen per licentie geanalyseerd zou moeten worden.

---

[31] EUHvJ 1 december 2011, C-145/10, Eva Maria Painer/Standard, §112-113.

[32] Zie art. 2 GPL v3, i.h.b.: 'You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force.'

3.3. Databankenwet

3.3.1. Wat is beschermd?

De Europese Databankenrichtlijn[33] definieert een databank als een verzameling van werken, gegevens of andere zelfstandige elementen, systematisch of methodisch geordend, en afzonderlijk met elektronische middelen of anderszins toegankelijk. De Nederlandse Databankenwet neemt deze definitie in de basis over, maar voegt er elementen aan toe die betrekking hebben op de voorwaarden waaronder de databank voor bescherming in aanmerking komt en is daardoor minder zuiver. De 'kale' Europese definitie is een ruime definitie die snel van toepassing zal zijn. Echter niet alle databanken genieten bescherming. Met betrekking tot databanken moet onderscheid gemaakt worden in drie beschermingsvormen:

- Eventuele auteursrechten die rusten op afzonderlijke elementen die in de databank zijn opgenomen. Bijvoorbeeld een databank met tekeningen van architecten. Een architect verliest uiteraard zijn auteursrecht niet indien zijn tekening in een databank wordt opgenomen.
- Eventuele auteursrechten op de structuur van de databank. De rangschikking en selectie van elementen kan auteursrechtelijk beschermd zijn, namelijk indien zij als een eigen intellectuele schepping van de maker van de databank hebben te gelden. Dit is over het algemeen een dunne bescherming. Alleen als de rangschikking of selectie tot uitdrukking komt in het door een derde overgenomene kan de maker daartegen optreden.
- Het *sui generis*-recht op de inhoud van de databank. Dit is bescherming van het geheel of een substantieel deel van de inhoud van de databank. Deze bescherming komt toe aan de producent van een databank die substantieel geïnvesteerd heeft in het verzamelen, verifiëren of presenteren van de inhoud van zijn databank.

Deze laatste vorm van bescherming zal hier verder besproken worden. De drempel om bescherming te verkrijgen is in vaste rechtspraak van het EU Hof van Justitie hoog gelegd, zoals blijkt uit onderstaand citaat uit het arrest Fixtures/Svenska Spel:[34]

> In dit verband moet […] het begrip investering in de verkrijging van de inhoud van een databank aldus worden opgevat dat het duidt op de middelen die worden aangewend om bestaande elementen te verkrijgen en in deze databank te verzamelen, met uitsluiting van de middelen die zijn aangewend voor het creëren van die elementen. […] strekt de door de richtlijn geregelde bescherming door het recht sui generis immers tot bevordering van de totstandkoming van systemen voor de opslag en verwerking van bestaande gegevens, en niet tot het creëren van gegevens die naderhand in een databank bijeen kunnen worden gebracht.

Aangezien lang niet alle investeringen meegeteld mogen worden wordt het moeilijker de drempel van de substantiële investering te halen. Niettemin is te verwachten dat veel van de grotere databanken die op Internet raadpleegbaar zijn wel degelijk bescherming ondervinden van het sui generis databankenrecht. De implicaties daarvan worden in de volgende subparagraaf beschreven.

3.3.2. Ruimte voor omgang met databanken

Het sui generis-databankenrecht kent twee exclusieve rechten toe aan de rechthebbende: het opvragingsrecht en het hergebruiksrecht. Het eerste is het recht om de inhoud van een databank of een substantieel deel daarvan permanent of tijdelijk over te brengen op een andere drager, ongeacht de wijze waarop en de vorm waarin dat gebeurt. Het hergebruiksrecht is het recht om de inhoud van een databank of een substantieel deel daarvan in enige vorm aan het publiek ter beschikking te stellen door verspreiding van exemplaren, verhuur, online transmissie of transmissie in een andere vorm. Men zou kunnen deken dat dan het opvragen of hergebruiken van niet substantiële delen van de inhoud van een databank vrij is (immers vallend buiten de exclusieve rechten van de maker). Dat is echter maar ten dele waar. Het exclusieve recht strekt zich ook uit over het herhaald en systematisch opvragen of hergebruiken van in kwalitatief of in kwantitatief opzicht niet-substantiële delen van de inhoud van een databank, wanneer dit in strijd komt met de normale exploitatie van die databank of ongerechtvaardigde schade toebrengt aan

[33] Richtlijn 96/9/EG van 11 maart 1996 betreffende de rechtsbescherming van databanken, PubEG van 27.3.96, L77/20.
[34] EUHvJ 9 november 2004, C-338/02 (Fixtures/Svenska Spel)

de rechtmatige belangen van de producent van de databank. Deze toevoeging moet voorkomen dat door herhaald en systematisch opvragen een databank wordt uitgemolken, dat wil zeggen dat langs deze weg de gehele inhoud of een substantieel deel daarvan verkregen wordt. Soms nemen houders van databanken ook technische maatregelen om dit uitmelken te voorkomen. Een voorbeeld is de site van de RDW die een gebruiker die te snel achter elkaar kentekengegevens opvraagt tijdelijk de toegang ontzegt (op basis van IP-adresblokkering). Het ontduiken van een dergelijke beveiliging – bijvoorbeeld door automatisch een wachttijd in te voeren voordat het volgende element uit de databank automatisch wordt opgevraagd – kan dus een inbreuk opleveren op het exclusieve recht van de houder van de databank.

Voor iRN/iColumbo-gebruikers is het databankenrecht relevant wanneer de gebruikte crawlers automatisch een substantieel deel van op het Internet toegankelijke beschermde databanken uitlezen, dan wel herhaald en systematisch niet-substantiële delen uitlezen. Denk in dit verband bijvoorbeeld aan het systematisch verzamelen van eBay-veilingpagina's of marktplaats.nl-advertenties over te koop aangeboden bedreigde diersoorten, vuurwapens of andere voorwerpen waarvan de handel illegaal is. De vraag is dan of zij daarvoor een licentie moeten verkrijgen van de databankrechthouder of onder een exceptie vallen. Art. 5 Databankenwet bevat een met art. 22 lid 2 Aw vergelijkbare beperking op het sui generis-recht:

> De rechtmatige gebruiker van een databank die op enigerlei wijze aan het publiek ter beschikking is gesteld mag zonder toestemming van de producent van de databank een substantieel deel van de inhoud van de databank […] opvragen of hergebruiken voor de openbare veiligheid of in het kader van een administratieve of rechterlijke procedure.

In welke mate eindgebruikers een beroep kunnen doen op deze exceptie, hangt af van de interpretatie van 'openbare veiligheid' en 'in het kader van een (…) procedure'; zie daarover onze opmerkingen hierboven betreffende art. 22 Aw.

3.4. Internationale aspecten

Het toepasselijk recht in het auteursrecht is het recht van het land waarvoor de rechthebbende zijn bescherming inroept. Indien vanuit Nederland een werk wordt opgevraagd bij een server in het buitenland (hetgeen bij iRN/iColumbo veelvuldig het geval zal zijn) en de rechthebbende daartegen bezwaar zou maken, dan is aannemelijk dat de rechthebbende bescherming vraagt voor het land waar de server staat, met name indien de desbetreffende informatie op de server niet specifiek op Nederland is gericht. Dat betekent dat buitenlands auteursrecht op de casus van toepassing kan zijn.

De meeste landen in de wereld hebben auteurswetgeving: 165 landen zijn aangesloten bij de Berner Conventie over auteursrecht, 89 landen zijn aangesloten bij het WIPO Copyright Treaty, dat specifiek gaat over de toepassing van het auteursrecht op werken in digitale vorm.[35]

Een snelle analyse van de auteurswetten in de verschillende EU-lidstaten leert dat zij niet alle een met art. 22 Aw vergelijkbare bepaling kennen die gebruik van werken ten behoeve van de openbare veiligheid of voor parlementaire, bestuurlijke en rechterlijke procedures toelaat. Art. 22 lid 2 Aw is weliswaar gebaseerd op een Europese richtlijn (zie art. 5(3)(e) Richtlijn 2001/29/EC) maar die richtlijn verplicht niet tot opname van een desbetreffende exceptie in het nationale auteursrecht. Ongeveer de helft van de EU-lidstaten heeft een bepaling die net als de Nederlandse bruikbaar is voor iRN- en iColumbo-doeleinden. Ongeveer een kwart heeft een bepaling die bruikbaar zou kunnen zijn, maar nadere voorwaarden stelt die mogelijk moeilijk te vervullen zijn. De rest kent een dergelijke exceptie niet.

Dat betekent dat het verzamelen van materiaal uit open bronnen die worden aangeboden vanuit landen die geen, of slechts een beperkte, exceptie hebben voor openbare veiligheid of bestuurlijke procedures, een zeker risico oplevert voor eindgebruikers om aangesproken te worden door auteursrechthebbenden. Deze zouden in de desbetreffende landen naar de rechter kunnen stappen en schadevergoeding vragen voor of een verbod op het zonder toestemming kopiëren van hun gegevens. Aangezien het gaat om publiek beschikbare gegevens en het kopiëren door eindgebruikers beperkt blijft (naar wij aannemen) tot intern gebruik, lijkt het ons onwaarschijnlijk dat auteursrechthebbenden in andere landen een procedure zouden beginnen tegen de eindgebruiker. Niettemin is het risico niet helemaal denkbeeldig dat bepaalde personen

[35] Zie http://www.wipo.int/treaties/en/.

of instanties, als het gebruik van iColumbo negatieve gevolgen voor hen zou kunnen hebben, bezwaar maken via de band van het auteursrecht op hun materiaal. Een goede inschatting van dit risico valt binnen het bestek van dit onderzoek moeilijk te geven; daarvoor is nader onderzoek nodig.

Voor het *sui generis* databankenrecht geldt eveneens dat het toepasselijk recht het recht is van het land waarvoor bescherming gevraagd wordt.[36] Anders dan bij het auteursrecht is het *sui generis* databankenrecht buiten de EU vrijwel onbekend. Als het toepasselijk recht het recht van een land buiten de EU is, dan is de kans klein dat daar niet-auteursrechtelijke bescherming bestaat voor databanken en dat haalt de angel uit de toepasselijkheid van dat recht. Een tweede verschil met het auteursrecht is dat het *sui generis*-recht beheerst wordt door het reciprociteitsbeginsel dat tot uitdrukking komt in overweging 56 bij de Databankenrichtlijn:

> Overwegende dat het recht van verbod op opvraging en/of hergebruik zonder toestemming niet van toepassing is op databanken waarvan de fabrikant onderdaan is van of zijn gewone verblijfplaats heeft in een derde land, en evenmin op databanken die zijn gemaakt door rechtspersonen die niet in een Lid-Staat gevestigd zijn in de zin van het Verdrag, tenzij dat derde land een vergelijkbare bescherming biedt voor databanken die zijn gemaakt door personen die onderdaan van een Lid-Staat zijn of hun gewone verblijfplaats op het grondgebied van de Gemeenschap hebben (...).

Aan databanken van buiten de EU wordt dus ook binnen de EU geen bescherming verleend, indien het land van de maker van de databank geen vergelijkbare bescherming biedt aan 'Europese' databanken. Zoals we hiervoor hebben gezien is dat meestal niet het geval. Voor zover de structuur van een databank of afzonderlijke elementen daaruit beschermd worden door het auteursrecht geldt uiteraard wel hetgeen hiervoor is gezegd over de internationale aspecten van het auteursrecht.

3.5. Korte blik op de toekomst

Hiervoor is de vraag opgeworpen of 'alles wat op Internet staat' beschermd zou worden door het auteursrecht, of om het anders te zeggen of het volle gewicht van het auteursrecht op (het gebruik van) *user-generated content* (UGC), tweets en blogs zou moeten drukken. Vooralsnog bestaan er geen specifieke regels hiervoor. Langzaamaan begint echter het besef te groeien dat op de genoemde inhoudscategorieën het auteursrecht niet onverkort toegepast behoort te worden, bijvoorbeeld indien (korte) werken van anderen in de inhoud verwerkt worden. De Europese Commissie zegt er het volgende over in haar communicatie over de interne markt voor intellectuele eigendomsrechten van mei 2011:

> There is a growing realisation that solutions are needed to make it easier and affordable for end-users to use third-party copyright protected content in their own works. Users who integrate copyright-protected materials in their own creations which are uploaded on the internet must have recourse to a simple and efficient permissions system. This is particularly pertinent in the case of "amateur" users whose UGC is created for non-commercial purposes and yet who face infringement proceedings if they upload material without the right holders' consent.[37]

In de tweede helft van 2012 zal de Europese Commissie een consultatie organiseren over *user-generated content*.[38] De Nederlandse regering zou willen dat de Commissie nog iets harder zou lopen voor UGC en ook de mogelijkheden voor introductie van een 'fair use'-achtige bepaling op Europees niveau zou verkennen. Vooralsnog geeft de Nederlandse regering haar Commissie Auteursrecht de opdracht om te onderzoeken welke mogelijkheden nu al bestaan onder het Europese recht om te komen tot een flexibelere omgang met UGC. De commissie heeft inmiddels geadviseerd dat de meest veelbelovende weg is om de citaatexceptie van art. 15a Aw op te rekken.

---

[36] Overweging 26 en art. 8(1) Verordening (EG) nr. 864/2007 van 11 juli 2007 betreffende het recht dat van toepassing is op niet-contractuele verbintenissen („Rome II").

[37] Communication from the Commission, A Single Market for Intellectual Property Rights Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe, Brussels, 24.5.2011, COM(2011) 287 final, par. 3.3.3, beschikbaar op: http://ec.europa.eu/internal_market/copyright/docs/ipr_strategy/COM_2011_287_en.pdf.

[38] *Kamerstukken II* 2011/12, 29 838, nr. 30, p.59.

In een speciaal rapport voor de VN wordt nog het volgende opgemerkt:[39]

> The Special Rapporteur welcomes initiatives taken in other countries to protect intermediaries, such as the bill adopted in Chile, which provides that intermediaries are not required to prevent or remove access to user-generated content that infringes copyright laws until they are notified by a court order. A similar regime has also been proposed in Brazil.

Ook in de wetenschap wordt nagedacht over de manier waarop het auteursrecht omgaat met UGC. Hugenholtz en Senftleben verkennen in een studie de mogelijkheden voor flexibelere toepassing van het auteursrecht.[40]

Juist op het gebied van de *user generated content* zal in de toekomst allicht het een en ander gaan veranderen. Voor zover er iets over te zeggen is over de inhoud van de verandering lijkt de discussie niet te gaan in de richting van het uitsluiten van auteursrechtelijke bescherming voor korte of kleine werken. De discussie gaat veeleer in de richting van het vergroten van de mogelijkheden om dergelijke werken te gebruiken terwijl ze auteursrechtelijk beschermd zijn.

3.6. Conclusie

De voor iRN/iColumbo belangrijkste wetgeving voor intellectueel eigendom bestaat de Auteurswet en de Databankenwet. Voor eindgebruikers betekent dit, dat zij oog moeten hebben voor de omstandigheden waaronder werken beschikbaar gesteld worden op het Internet.

- Heeft een website 'terms of use' die iets zeggen over het gebruik van de werken en databanken die op de website staan? Worden ze bijvoorbeeld onder een creative commons-licentie beschikbaar gesteld? Dan valt al aanstonds te lezen welk gebruik is toegestaan. Dat is met name interessant als het toegestane gebruik het gebruik van iRN/iColumbo zou omvatten.
- Ziet de website er uit als een website waarop werken legaal (bijvoorbeeld door de rechthebbende zelf of met diens toestemming) beschikbaar worden gesteld om te downloaden? In geval van een 'legale' webpagina kan vertrouwd worden op een impliciete licentie voor het binnenhalen van het materiaal. Is de website 'illegaal' dan wordt het kritischer. Ook wanneer materiaal weliswaar door de rechthebbende op Internet wordt gepubliceerd maar niet als zodanig voor derden om van het Internet af te halen, is het dubieus of men een impliciete licentie mag aannemen. In die gevallen moet dan terugvallen op beperkingen van het auteursrecht, waarbij met name art. 22 lid 2 Aw relevant is. Dan wordt men afhankelijk van de interpretatie van die bepalingen (wat is een bestuurlijke procedure? wat is openbare veiligheid?), waarover momenteel weinig eenduidigheid bestaat.

De eindgebruikers moeten voorts oog hebben voor het gebruik dat ze maken van de werken.

- Indien de werken na download gedeeld worden in een grote groep van personen dan zal zulks in het algemeen relevant zijn onder de auteursrechten en databankrechten die op het materiaal van toepassing zijn. De gebruiksintensiteit van een (in ruime kring gedeeld) werk maakt het moeilijker om het gebruik te rechtvaardigen: *terms of use* en impliciete licenties zullen hier weinig helpen. Vertrouwen op wettelijke beperkingen wordt daarbij misschien moeilijker vanwege de driestappentoets van art. 5 lid 5 Richtlijn 2001/29/EG.
- Bewerkingen van werken zoals vertalingen zijn relevante handelingen onder het auteursrecht. Onduidelijk is of zij ook onder de beperking ten behoeve van de openbare orde of bestuurlijke procedures gebracht kunnen worden.

De gevolgen van auteurs- en databankenrecht voor eindgebruikers hebben een weerslag op de systeemontwikkeling. Aangezien voor eindgebruikers het binnenhalen van materiaal gemakkelijker te rechtvaardigen is dan het daarop volgende gebruik, zoals (her)verspreiding en vertaling, zou het systeem dit kunnen reflecteren, zo mogelijk door vervolggebruik niet te ondersteunen of onmogelijk te maken, dan wel door de gebruiker te waarschuwen wanneer modules bewerkingen van materiaal maken.

Duidelijk is verder dat er de nodige open vragen overblijven, die in het bestek van dit onderzoek niet uitgebreid konden worden onderzocht. Met name de betekenis van de termen

[39] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council (16 mei 2011) UN Doc A/HRC/17/2, §43 (met weglating van voetnoten).
[40] Hugenholtz & Senftleben 2011.

‘openbare veiligheid’ en ‘bestuurlijke procedure’ in art. 22 Aw en ‘administratieve procedure’ in art. 5 Databankenwet, alsook de vraag of het bewerken en vertalen van materiaal onder de term ‘overnemen’ uit art. 22 Aw te begrijpen is, verdienen nader onderzoek. Dat geldt ook voor de implicaties van auteurswetten die in het buitenland (zowel de nodige EU-lidstaten als andere landen) gelden wanneer die geen wettelijke exceptie zoals art. 22 Aw kennen.

4. Wetgeving met betrekking tot eindgebruikers

4.1. Politie

De politie gebruikt op grote schaal iRN en zal ook iColumbo gaan gebruiken. Hierbij kan de afkomst (vanuit een politie-pc) afgeschermd worden. Het doel kan zijn algemeen surveilleren in het kader van de handhaving van de openbare orde, of doelgerichte opsporing in het kader van een concreet onderzoek.

4.1.1. Grondslag voor bevoegdheden

Art. 2 Politiewet of stelselmatige observatie?

De grondslag op basis waarvan de politie Internetonderzoek in open bronnen kan doen, wordt veelal gezocht in art. 2 Politiewet 1993: 'De politie heeft tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.' Op basis van dit artikel zijn geringe inbreuken op grondrechten van burgers toegestaan.[41] Voor zwaardere inbreuken op grondrechten is echter een expliciete bevoegdheid nodig. Maakt politieonderzoek in open bronnen een dusdanige inbreuk op de privacy van burgers dat art. 2 PolW niet meer als grondslag kan gelden? Zo ja, dan heeft dat consequenties voor de inzet van het middel: het mag dan alleen voor opsporing maar niet voor de algemene politietaak worden ingezet.

Het verzamelen van persoonsgegevens van het Internet raakt de privacy van burgers en valt onder art. 8 EVRM.[42] Dat gegevens zich in de openbaarheid bevinden, doet daar niet aan af: ook in publieke ruimten bestaat een zekere mate van redelijke privacyverwachting.[43] Bovendien leveren zoekopdrachten in open bronnen ook gegevens op die anderen over iemand hebben gepubliceerd, wat privacygevoelige informatie kan betreffen. Maar omdat de gegevens publiekelijk toegankelijk zijn, leveren zoekacties in open bronnen mogelijk een geringe inbreuk op de privacy op, waarvoor art. 2 PolW dan een toereikende wettelijke grondslag kan bieden. Dat hangt er echter wel van af hoe het systeem wordt gebruikt.

Wanneer systematisch en grootschalig gegevens worden verzameld, zeker bij een gerichte zoekactie op een bepaalde persoon, kan een groot deel van de persoonlijke levenssfeer van die persoon in kaart worden gebracht. Tegenwoordig staat immers zoveel op Internet dat een bijzonder nauwkeurig profiel van iemand ontstaat: adresgegevens, interesses, meningen, foto's, lidmaatschap van verenigingen, en wat niet al. In zulke gevallen krijgt het onderzoek het karakter van stelselmatige observatie (art. 126g Sv)[44]. Bepalend voor het stelselmatige karakter van de observatie is of deze 'tot resultaat [kan] hebben dat een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven'.[45] Het hoeft daarbij niet om het leeuwendeel van iemands persoonlijke leven te gaan dat in beeld komt; wanneer een min of meer volledig beeld ontstaat van *onderdelen* van het privéleven, zoals iemands sociale contacten met vrienden, zijn uitgaansleven of zijn verenigingsleven, krijgt de observatie een stelselmatig karakter. De Memorie van Toelichting geeft aan aantal aanknopingspunten om dit verder in te vullen:

> de duur, de plaats, de intensiteit of frequentie en het al dan niet toepassen van een technisch hulpmiddel dat méér biedt dan alleen versterking van de zintuigen. Ieder voor zich, maar met name in combinatie, zijn deze elementen bepalend voor de vraag of een min of meer volledig beeld van

[41] Zie bijvoorbeeld HR 20 januari 2009, LJN BF5603.
[42] Vgl. De Hert en Gutwirth 2009.
[43] Vgl. EHRM 24 juni 2004 (Hannover t. Duitsland), App.nr. 59320/00, §77; EHRM 25 oktober 2007 (Van Vondel t. Nederland), App.nr. 38258/03, §48.
[44] Afhankelijk van het type onderzoek (naar beraamde of gepleegde georganiseerde misdaad of terroristische misdrijven) kan in plaats van art. 126g art. 126o of 126zd Sv van toepassing zijn. Waar dit rapport spreekt van de BOB-bevoegdheden in art. 126g e.v. Sv (titel IVa) moeten mutatis mutandis ook de bevoegdheden uit Titel V en VB worden gelezen.
[45] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26-27.

> bepaalde aspecten van iemands leven wordt verkregen. (...) Een normale surveillance zal geen vorm van stelselmatige observatie zijn. Ook het oppervlakkig in de gaten houden van bijvoorbeeld een groep jongeren zal doorgaans geen stelselmatige observatie zijn. Wanneer echter een persoon intensief of frequent wordt gevolgd, zal wel sprake zijn van stelselmatige observatie.[46]

Wanneer valt openbrononderzoek nu onder stelselmatige observatie? Hoewel de 'plaats' (open bronnen op Internet) tegen een kwalificatie van stelselmatige observatie pleit, pleit het gebruik van technische hulpmiddelen eerder vóór een dergelijke kwalificatie. '*Al heel snel* zal bij gebruik van technische hulpmiddelen sprake zijn van stelselmatige observatie, maar er zijn situaties denkbaar dat dat niet het geval is'.[47] Dat laatste slaat vooral op verrekijkers of handmatig bediende camera's die alleen een versterking van de zintuigen bieden. Bij zoekacties op Internet kunnen aanzienlijk meer gegevens te verzamelen dan met menselijk oog en oor zijn waar te nemen. Zeker wanneer de gegevensverzameling geautomatiseerd plaatsvindt en wanneer modules worden gebruikt, wat bij iColumbo het geval is, om gegevens in standaardformaat om te zetten ten behoeve van automatische gegevensvergelijking, is er sprake van een 'technisch hulpmiddel dat (…) meer mogelijkheden biedt'. Bovendien worden gegevens ook opgeslagen (en mogelijk voor langere tijd bewaard), wat de inbreuk op de persoonlijke levenssfeer vergroot.[48]

Het zal dan van de frequentie en intensiteit afhangen of daadwerkelijk sprake is van stelselmatige observatie. Wanneer langdurig, hoogfrequent en/of op uiteenlopende plaatsen op het Internet op dezelfde persoon wordt gezocht, dan gaat de observatie vermoedelijk het karakter van een geringe inbreuk op de privacy te boven. Wanneer bij openbrononderzoek op Internet veel verschillende (openbare) plaatsen worden geobserveerd,[49] is de kans veel groter dat een min of meer volledig beeld van een bepaald aspect van iemands persoonlijke leven in kaart wordt gebracht.

Hoewel de rechtspraak over stelselmatige observatie vrij liberaal is (vaak is art. 2 Politiewet voldoende), bestaat er een risico dat een rechter, vanwege het gebruik van technische hulpmiddelen en de intensiteit van het zoeken in uiteenlopende Internetbronnen, openbrononderzoek op Internet toch als stelselmatige observatie zal aan merken. Wanneer de politie bij een opsporingsonderzoek intensiever gebruik maakt van iColumbo, valt het aan te raden daarvoor een bevel van de officier van justitie ex art. 126g Sv te vragen.

Wanneer de politie surveilleert op Internet – dus wanneer er geen redelijk vermoeden van een strafbaar feit of aanwijzing van een terroristisch misdrijf bestaat – is slechts een geringe inbreuk op de privacy toegestaan; dat betekent dat bij surveilleren zeer terughoudend gebruik moet worden gemaakt van iColumbo om gegevens over specifieke personen uit verschillende bronnen te verzamelen en geautomatiseerd te combineren.

Afschermen van afkomst: stelselmatig inwinnen van informatie?

Bij de Wet BOB is een andere bevoegdheid ingevoerd, het stelselmatig inwinnen van informatie over de verdachte door een opsporingsambtenaar 'zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar' (art. 126j Sv). Deze bevoegdheid betreft vooral politiële informanten, die (in burger) gesprekken voeren met verdachte en zijn omgeving om informatie in te winnen. Dat is minder direct toepasbaar op openbrononderzoek op Internet dan stelselmatige observatie, aangezien er alleen bestaande gegevens worden verzameld en niet naar gegevens wordt gevraagd. Maar de toelichting bij deze bepaling is wel relevant: met het element 'zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar'

> is duidelijker aangegeven welk aspect van deze opsporingsmethode met zich meebrengt dat een wettelijke basis vereist is: het aspect van misleiding. Die misleiding is belastend voor de verdachte waarmee gesprekken gevoerd worden; ook het stelselmatig inwinnen van informatie bij mensen in de

[46] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 27.
[47] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 110 (cursivering toegevoegd).
[48] Buruma 2001, p. 34. Vgl. EHRM 28 oktober 1994, NJ 1995, 509 (Murray t. Verenigd Koninkrijk); EHRM 4 december 2008, App.nrs. 30562/04 en 30566/04 (S. en Marper t. Verenigd Koninkrijk).
[49] Dat is een belangrijk verschil met veel jurisprudentie over stelselmatige observatie, die meestal betrekking heeft op statische observatie op één plaats. Zie bijv. HR 29 maart 2005, LJN AS2752; HR 26 oktober 2010, LJN BN0004.

omgeving van de verdachte, terwijl de opsporingsambtenaar niet als zodanig herkenbaar is, is echter misleidend en behoeft een wettelijke grondslag.[50]

Wanneer een gebruiker van iRN of iColumbo de IP-informatie afschermt, zodat beheerders van webpagina's niet kunnen zien dat een bezoeker afkomstig is van een met de politie geassocieerd IP-adres, lijkt er sprake te zijn van een vergelijkbare vorm van misleiding als bij politiële informanten. De verdachte en personen in diens omgeving zien immers niet dat de politie bij hen gegevens aan het vergaren is.[51] Het enige verschil is dat bij politiële informanten aan de personen actief informatie wordt ontlokt, terwijl bij openbrononderzoek de personen uit zichzelf informatie beschikbaar stellen.[52] Is dat verschil voldoende significant om te stellen dat er geen ontoelaatbare misleiding plaatsvindt? Als bij politieel openbrononderzoek de afkomst van de zoekactie bewust en stelselmatig wordt afgeschermd, juist om te voorkomen dat verdachten of personen in hun omgeving merken dat de politie naar informatie over hen op zoek is, is de uitspraak van de wetgever van toepassing: 'De verdachte zal niet verwachten dat de informatie die hij prijs geeft, wordt gebruikt voor opsporingsdoeleinden. De opsporingsambtenaar misleidt de verdachte.'[53] Daarom kan men stellen dat ook een expliciete wettelijke grondslag nodig is voor zoekacties van een politiefunctionaris in iRN en iColumbo 'zonder dat kenbaar is dat hij optreedt als opsporingsambtenaar'. Die grondslag is dan hetzij stelselmatige observatie (art. 126g Sv) hetzij stelselmatig inwinnen van informatie (art. 126j Sv), waarvoor een bevel van de officier van justitie nodig is. Voor beide bevoegdheden geldt dat het moet gaan om verdenking van een misdrijf (dan wel aanwijzingen van een terroristisch misdrijf). Openbrononderzoek met afgeschermde IP-afkomst voor handhaving van de openbare orde, zoals surveilleren op Internet, is volgens deze interpretatie niet toegestaan. Bij gebreke van jurisprudentie over inwinnen van informatie op Internet is het onduidelijk of de rechtspraak deze interpretatie, met nadruk op het misleidende element, zal hanteren, of meer nadruk zal leggen op het niet-interfererende karakter van de informatie-inwinning. Een uitspraak van de wetgever hierover zou wenselijk zijn. Tot die tijd kan de opsporingsambtenaar die zijn IP-afkomst wil afschermen, het zekere voor het onzekere nemen en een bevel van de officier vragen.

Registratie bij semi-open bronnen

Onder onderzoek in 'open bronnen' verstaan sommigen ook het onderzoek in webpagina's die zijn afgeschermd, bijvoorbeeld pagina's waarvoor een registratie nodig is of socialenetwerkpagina's die alleen voor (vrienden van) vrienden toegankelijk zijn. Zolang er geen dwangmiddel wordt ingezet, zou openbrononderzoek mogelijk ook dergelijke pagina's kunnen omvatten. De opsporingsambtenaar kan zich registreren, onder eigen naam of onder pseudoniem, en vervolgens de gegevens verzamelen.

Aangezien het gaat om afgeschermde pagina's, is de inbreuk op de privacy hier in principe groter – de gebruikers hebben allicht een hogere privacyverwachting omdat de gegevens alleen na registratie toegankelijk zijn, wat onder andere ook betekent dat ze veelal niet direct via zoekmachines te vinden zijn. Daarom zal onderzoek in afgeschermde bronnen vrijwel altijd verder gaan dan wat toegestaan is op basis van art. 2 PolW.

Daar komt bij dat wanneer een opsporingsambtenaar bij de registratie een pseudoniem gebruikt, hij mogelijk ook de gebruikers van het afgeschermde forum misleidt, in de zin dat hij informatie verzamelt zonder dat hij als opsporingsambtenaar kenbaar is. Evenals bij het afgeschermd onderzoek van vrij toegankelijke bronnen (zie boven), lijkt daarom een expliciete wettelijke grondslag nodig wanneer de politieambtenaar zijn identiteit afschermt bij registratie in semi-open bronnen. Het aanmaken van een profielpagina in bijvoorbeeld Hyves of Facebook onder een andere naam en zonder verwijzing naar de rol van opsporingsambtenaar is dan niet

[50] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 62. Daarom is misleiding een zelfstandige basis om de bevoegdheid wettelijk te regelen, ook als het gaat om lichte inbreuken op de privacy; '[z]odra sprake is van misleiding lijkt art. 126j te moeten worden toegepast', aldus T&C Sv, art. 126j Sv, aant. 3(b) en (c).

[51] Vgl. Buruma & Verborg 2008, aant. 8: ook het verzamelen van niet-persoonsgebonden informatie, zoals over witwasmethodieken of smokkelroutes, kan 'gepaard gaan met misleiding van degenen bij wie de informatie wordt ingewonnen. In dergelijke gevallen verdient afgifte van een bevel, omwille van de integriteit van de opsporing, daarom toch de voorkeur'.

[52] 'De opsporingsambtenaar observeert dus niet alleen, maar interfereert actief in het leven van de verdachte. Hij gaat daarbij verder dan alleen waarnemen of luisteren.' *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 35.

[53] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 30.

toegestaan op basis van art. 2 PolW.[54] (Dit ligt wellicht anders als het profiel duidelijk een onzinprofiel is, bijvoorbeeld met naam en foto van Daffy Duck; in dat geval is de misleiding in zichzelf al duidelijk kenbaar.) Ook daarvoor is dan een bevel nodig van de officier ex art. 126g (stelselmatige observatie) dan wel, als de opsporingsambtenaar actief gaat meedoen in het forum, ex art. 126j (stelselmatig inwinnen van informatie), of zelfs ex 126h als het meedoen overgaat in infiltratie.

4.1.2. Eisen aan gebruik van bevoegdheden

Als iColumbo wordt gebruikt op basis van art. 2 PolW (wat zoals boven aangegeven alleen met grote terughoudendheid en in beperkte omvang mag), zijn er geen specifieke procedurele vereisten. Als de basis is de bevoegdheid van stelselmatige observatie of stelselmatige informatie-inwinning, gelden de reguliere eisen die in art. 126g lid 4-8 en 126j lid 2-5 staan. Belangrijk is vooral een schriftelijk bevel van de officier met vermelding van de feiten en omstandigheden die een verdenking van misdrijf opleveren, de verdachte en de geldigheidsduur en wijze van uitvoering. Bij dat laatste is het aan te bevelen een aanduiding te geven van de reikwijdte van het beoogde onderzoek via iColumbo, bijvoorbeeld in welke (typen) bronnen moet worden gezocht, op welke personen of welke categorieën trefwoorden, met welke frequentie en hoe lang.

Tijdens de workshop met eindgebruikers werd naar voren gebracht dat tijdens iColumbo-gebruik de verbaliseringsplicht (art. 152 Sv) een complicatie kan zijn, met name wanneer en passant feiten naar boven komen die mogelijk strafrechtelijk relevant zijn hoewel het onderzoek daar niet specifiek op was gericht. Moet van elk mogelijk strafbaar feit waarvan bij een zoekactie indicaties blijken, proces-verbaal worden opgemaakt? Dat valt niet algemeen te beantwoorden. Belangrijk is dat de opsporingsambtenaar steeds de achterliggende reden van de verbaliseringsplicht voor ogen houdt, namelijk dat 'geverbaliseerd wordt wat, als de zaak naar verwachting tot een strafrechtelijke afdoening leidt, voor een later oordelende rechter van belang is. Ook dient steeds proces-verbaal te worden opgemaakt als een klacht op grond van artikel 12 Sv een reële mogelijkheid is.'[55] De Wet herziening regels betreffende de processtukken in strafzaken[56] kan soelaas bieden, nu de officier van justitie de bevoegdheid krijgt te bepalen dat verbalisering achterwege kan blijven (nieuw art. 152 lid 2 Sv). Het OM zou bijvoorbeeld richtlijnen kunnen opstellen voor de reikwijdte van de verbaliseringsplicht bij gebruik van iColumbo; ook kan een officier voor concrete onderzoeken aanwijzingen geven wat wel en niet geverbaliseerd moet worden tijdens het gebruik van iColumbo.

4.1.3. Besluit technische hulpmiddelen

Als iColumbo wordt gebruikt op basis van de bevoegdheid van stelselmatige observatie of stelselmatige informatie-inwinning, heeft dat ook consequenties voor het gebruik van de technische hulpmiddelen. Aangezien iColumbo, evenals iRN, een technisch hulpmiddel is dat meer biedt dan alleen versterking van de zintuigen, zal de officier bij zijn bevel tot stelselmatige observatie of informatie-inwinning moeten bepalen dat iColumbo als technisch hulpmiddel wordt gebruikt (art. 126g lid 3 Sv). Volgens art. 126ee Sv is dan het Besluit technische hulpmiddelen[57] van toepassing op iColumbo. Dit besluit bevat, in de woorden van art. 126ee Sv, regels omtrent:

a. de opslag, verstrekking en plaatsing van de technische hulpmiddelen, bedoeld in de artikelen 126g, derde lid (…);

b. de technische eisen waaraan de hulpmiddelen voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde waarnemingen;

c. de controle op de naleving van de eisen, bedoeld onder b;

d. de instellingen die de registratie van signalen aan een technische bewerking onderwerpen;

[54] Vgl. Buruma & Verborg 2008, aant. 3: 'Maar misleiding kan zich voordoen als deze undercover in strijd met de waarheid antwoordt dat hij geen opsporingsambtenaar is en zo verder kan deelnemen aan een chatsessie. Als misleiding van de overige deelnemers voorzienbaar is, verdient afgifte van een bevel de voorkeur.'
[55] *Kamerstukken II* 2009/10, 32 468, nr. 3, p. 6.
[56] Stb. 2011, 611.
[57] *Stb.* 2006, 524.

e. de wijze waarop de bewerking, bedoeld onder d, plaatsvindt met het oog op de controleerbaarheid achteraf, dan wel de waarborgen waarmee deze is omgeven en de mogelijkheden voor een tegenonderzoek.

Uit een keuringsrapport moet blijken dat de technische hulpmiddelen voldoen aan eisen van automatische registratie van datum/tijd, beveiliging en niet-manipuleerbare opslag.[58] Sommige eisen van het Besluit, zoals eisen voor opslag, verstrekking en plaatsing van technische hulpmiddelen (hfd. 2 Besluit technische hulpmiddelen), zijn echter meer toegespitst op fysieke hulpmiddelen dan op programmatuur, en het is niet duidelijk hoe deze eisen toepasbaar zijn op systemen als iRN/iColumbo. Andere functionele eisen van het Besluit (zoals beveiliging en niet-manipuleerbaarheid) wel toepasbaar; het zijn al ontwerpeisen van het iColumbo-systeem, zodat het systeem mogelijk toch kan worden goedgekeurd als technisch hulpmiddel als de 'fysieke eisen' als niet van toepassing kunnen worden beschouwd. Of en hoe iRN/iColumbo kan worden getoetst aan de eisen van het Besluit – bijvoorbeeld door functionele interpretatie van het Besluit zelf in de reguliere procedure, of door een alternatief keuringsrapport van een EDP-audit-achtige instantie die dezelfde functionele eisen, maar dan toegespitst op programmatuur, toetst – moet nader worden uitgezocht. Naar verwachting zal een momenteel lopend onderzoek van de Radboud Universiteit naar waarborgen voor de betrouwbaarheid en beveiliging van het iRN/iColumbo-systeem goede aanknopingspunten kunnen bieden om aan de functionele eisen van het Besluit tegemoet te komen.

In elk geval is wel belangrijk dat binnen redelijke termijn in een keuringsrapport voor iRN/iColumbo wordt voorzien, om te waarborgen dat met iColumbo verkregen materiaal bruikbaar is als bewijs in de rechtszaal.

4.1.4. Internationale aspecten

Omdat onderzoek in open bronnen zich nauwelijks tot Nederlands grondgebied kan beperken, is het nodig kort in te gaan op de vraag onder welke voorwaarden de politie in buitenlandse bronnen op het Internet mag zoeken. Hiervoor is vooral art. 32(a) van het Cybercrime-Verdrag (CCV) van belang: 'Een Partij kan, zonder de toestemming van een andere Partij: a. zich toegang verschaffen tot opgeslagen publiekelijk toegankelijke (open bron) computergegevens, ongeacht waar deze zich in geografisch opzicht bevinden'. Verdragspartijen kunnen dus zonder autorisatie openbrononderzoek doen naar data opgeslagen op computers in andere verdragspartijen.[59] Moet de politie bronnen uit niet-verdragspartijen (waaronder België, Oostenrijk en Rusland) mijden? Deze zouden het binnenhalen door buitenlandse politie van gegevens opgeslagen op hun territorium, ook al zijn deze publiek beschikbaar, als een inbreuk op hun soevereiniteit kunnen beschouwen waarvoor toestemming van de staat nodig is. Het is echter onwaarschijnlijk dat een buitenlandse staat problemen zal maken indien de politie zonder verdragsbasis in die staat opgeslagen, publiek toegankelijke gegevens verzamelt.

Wat precies onder 'publiek toegankelijke (open bron)' moet worden verstaan is niet duidelijk. Het gaat in elk geval om onderzoek waarbij geen dwangmiddel of medewerking van derde partijen nodig is. De literatuur noemt vooral webpagina's die zonder toegangscontrole te bezoeken zijn,[60] maar mogelijk vallen ook semi-open Internetbronnen onder de bepaling die publiekelijk na registratie toegankelijk zijn.

4.1.5. Wet politiegegevens

Op verwerking van persoonsgegevens door de politie is niet de Wbp maar de Wet politiegegevens (WPolG) van toepassing. Deze wet is onlangs aangepast aan het Europese Kaderbesluit over politiële en justitiële dataprotectie.[61] Deze wet is van toepassing op de verwerking van politiegegevens ('elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt') die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen (art. 2). Een bestand is 'elk gestructureerd geheel van politiegegevens (…) dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen' (art. 1 onder p). Zoekacties via iColumbo leiden tot opslag van persoonsgegevens van verschillende

[58] Art. 18 j° art. 10, 12, 13 en 14 Besluit technische hulpmiddelen.
[59] Zie http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (geraadpleegd 31 januari 2012) voor een overzicht van de momenteel 32 verdragspartijen.
[60] Zie bijv. Walden 2007, p. 318.
[61] *Stb.* 2011, 490, inwerkingtreding 1 april 2012 (Stb. 2012, 129).

personen; het ligt in de rede dat de opslag dusdanig gebeurt dat het een gestructureerd geheel betreft waarop verdere zoekacties en bewerkingen ('volgens bepaalde criteria') mogelijk zijn. Dat betekent dat het gebruik van iColumbo onder de WPolG valt.

De verwerking van persoonsgegevens is dan gebonden aan diverse wettelijke eisen. De gegevens moeten 'terzake dienend en niet bovenmatig' zijn (art. 3 lid 2), wat suggereert dat enige terughoudendheid nodig is bij grootschalige zoekacties in open bronnen. Gevoelige persoonsgegevens, zoals gegevens betreffende ras of gezondheid, mogen alleen worden verzameld als dit *onvermijdelijk* is voor het doel dat wordt beoogd (art. 5 WPolG). Aangezien foto's van personen informatie kunnen opleveren over ras of gezondheid, worden foto's haast per definitie beschouwd als gevoelige persoonsgegevens;[62] daarom moet de politie zeer terughoudend zijn met het geautomatiseerd verzamelen en verwerken van foto- en videomateriaal uit open bronnen. Verder moet de verantwoordelijke (degene die het doel bepaalt van een iColumbo-onderzoek) maatregelen treffen om ervoor te zorgen dat de verzamelde gegevens 'juist en nauwkeurig' zijn (art. 4 lid 1), wat een zorgplicht oplevert om richtlijnen op te stellen voor de omgang met openbronmateriaal, dat uit zichzelf weinig aanspraak kan maken op een kwalificatie als juistheid of nauwkeurigheid. Verder moeten de gegevens vanzelfsprekend, vergelijkbaar met de Wbp (zie par. 2.2), op passende wijze worden beveiligd (art. 4 lid 3).

Vooral doelbinding is een belangrijke randvoorwaarde voor openbrononderzoek, zeker nu de gewijzigde Wet politiegegevens scherpere eisen stelt: verwerking voor andere doeleinden dan waarvoor gegevens zijn verzameld mag alleen 'voor zover [de WPolG] daar uitdrukkelijk in voorziet, deze verwerking niet onverenigbaar is met het doel waarvoor deze gegevens zijn verkregen en de verwerking voor dat andere doel overigens noodzakelijk is en in verhouding staat tot dat doel. De verdere verwerking is alleen mogelijk door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang zijn aangewezen' (art. 3 lid 3). Dat betekent dat politiediensten zorgvuldig vooraf het doel van openbrononderzoek moeten overdenken en specificeren.

Gegevens moeten worden verwijderd als ze niet langer noodzakelijk zijn of wettelijk moeten worden bewaard (art. 4 lid 2), maar de bewaartermijn verschilt per type onderzoek. Gegevens verzameld ter uitvoering van de dagelijks politietaak mogen één jaar worden gebruikt (art. 8 lid 1); daarna mogen ze maximaal 5 jaar blijven opgeslagen om te worden vergeleken met nieuwe politiegegevens of om onderlinge verbanden te vinden (art. 8 lid 6 j^{o} lid 2 en 3); gegevens verzameld via iColumbo voor de dagelijke politietaak mogen dus maximaal zes jaar worden bewaard en gebruikt voor *data mining*. Als iColumbo wordt gebruikt 'met het oog op de handhaving van de rechtsorde in een bepaald geval',[63] moet het doel daarvan schriftelijk worden vastgelegd; deze gegevens mogen worden gebruikt zolang ze nodig zijn voor dit doel, en daarna nog maximaal een half jaar worden bewaard voor het geval ze relevant blijken voor een ander onderzoek (art. 9). Gegevens verzameld voor een onderzoek om inzicht te verkrijgen 'in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde' (zoals georganiseerde of zeer zware misdrijven) mogen langer worden bewaard, namelijk tot 'vijf jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van de politiegegevens' (art. 10). Voor de inrichting van het systeem van iColumbo is bij dit alles nog relevant dat gegevens die op grond van deze bepalingen worden verwijderd, nog vijf jaar na verwijdering bewaard moeten blijven 'ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen' (art. 14 lid 1); ze mogen dan dus niet meer worden gebruikt voor politieonderzoek, maar moeten nog wel ergens beveiligd opgeslagen blijven.

Verder zijn de bepalingen voor geautomatiseerde vergelijking en in combinatie zoeken relevant voor iColumbo. Binnen de dagelijkse politietaak kan dit op basis van art. 8 lid 2-3; voor handhaving van de rechtsorde in een concreet geval, zoals een opsporingsonderzoek, en voor onderzoek naar ernstige bedreigingen van de rechtsorde, is *data mining* mogelijk op basis van

[62] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 105; Hoge Raad 23 maart 2010, LJN BK6331. Zie over deze problematiek Zwenne & Mommers 2010.

[63] 'De handhaving van de rechtsorde kan aan de orde zijn bij een opsporingsonderzoek, bij een verkennend onderzoek en zodra bijzondere opsporingsmethoden worden ingezet. Het moment waarop sprake is van een gerichte verwerking zal veelal samengaan met het moment waarop om opsporingstechnische of tactische redenen aanleiding bestaat de gegevens binnen de politie af te schermen', Aanwijzing Wet politiegegevens, Stcrt. 2008, 142.

art. 11. Daarvoor moeten de opsporingsambtenaren specifiek zijn geautoriseerd, waarvoor in aanmerking komen 'de ambtenaren van politie die zijn belast met taken of werkzaamheden op het gebied van de coördinatie van het informatieproces ter ondersteuning van een goede uitvoering van de politietaak' (art. 2.1 en 2.2 Besluit politiegegevens). Als het nodig is voor de goede uitvoering van de gegevensvergelijking, kan de leider van het desbetreffende onderzoek of zijn plaatsvervanger de gegevens voorzien van een code 'instemming verdere verwerking' of 'vertrouwelijke verwerking' (zie nader art. 2.12 Besluit politiegegevens). Deze codering heeft gevolgen voor de manier waarop gevonden verbanden tussen gegevens voor gebruikers zichtbaar gemaakt mogen worden (zie daarover art. 2.11 Besluit politiegegevens).

De mogelijkheid om gegevens te markeren is overigens ook relevant in het kader van inzagerechten. Op basis van art. 25 WPolG heeft iedereen de mogelijkheid om bij de verantwoordelijke (degene binnen de politie die het doel van iColumbo-gebruik bepaalt) na te vragen of politiegegevens over hem of haar zijn vastgelegd. Kennisneming kan worden onthouden als dat noodzakelijk is voor de goede uitvoering van de politietaak, gewichtige belangen van derden, of de veiligheid van de staat (art. 27). Aangezien bij iColumbo-gebruik gegevens van vele Nederlanders kunnen worden vastgelegd, is het belangrijk te bepalen in welke gevallen de politie een uitzonderingsgrond kan inroepen; in het algemeen lijkt ons niet dat als een Nederlandse burger vraagt of zij in het iColumbo-systeem is vastgelegd, kennisneming kan worden geweigerd vanwege de goede uitvoering van de politietaak. Binnen het bestek van dit onderzoek kunnen we niet de reikwijdte van de inzagerechten onderzoeken; nader onderzoek en beleid op dit punt zijn wenselijk. In elk geval is voor de functionaliteit van iColumbo van belang dat eenvoudig achterhaald kan worden of iemand staat geregistreerd en dat het technisch mogelijk is om de gegevens over iemand te corrigeren, aan te vullen of te verwijderen. Ook kan een betrokkene vragen om gegevens af te schermen, dat wil zeggen de gegevens markeren 'met als doel de verwerking ervan in de toekomst te beperken' (art. 1 onder n).

4.1.6. Korte blik op de toekomst

Er zijn ons geen aanhangige wetsvoorstellen bekend die relevant zijn voor de vraagstukken van wettelijke grondslag of de eisen die aan uitoefening van bevoegdheden worden gesteld. In bovenstaande zijn we reeds uitgegaan van de aanstondse wijziging betreffende de verbaliseringsplicht.

Op de iets langere termijn zal de Wet politiegegevens moeten worden aangepast aan het herziene Europeesrechtelijke kader voor gegevensbescherming. Het Kaderbesluit voor verwerking van politiële en justitiële persoonsgegevens wordt vervangen door een Richtlijn, waarvoor in januari 2012 een eerste voorstel werd gepubliceerd.[64] Op dit moment valt niet te voorzien hoe de uiteindelijke richtlijn eruit zal zien. Voor iColumbo relevante onderdelen van het richtlijnvoorstel die mogelijk op termijn tot een wijziging van het Nederlandse recht zouden kunnen leiden zijn:

- de eis dat politiële gegevens waar nodig geactualiseerd worden ('where necessary, kept up to date', art. 4(d) Richtlijnvoorstel);
- de mogelijkheid om gevoelige persoonsgegevens (zoals foto's) te verwerken als deze gegevens ontwijfelbaar door de persoon zelf publiek zijn gemaakt ('data which are manifestly made public by the data subject', art. 8(2)(c) Richtlijnvoorstel);
- de eis dat de verantwoordelijke zoveel mogelijk een duidelijk onderscheid maakt tussen verschillende categorieën personen, namelijk verdachten, veroordeelden, slachtoffers, getuigen, contacten van verdachten en veroordeelden, en overige personen (art. 5 Richtlijnvoorstel);
- de eis dat bij de verwerking onderscheid wordt gemaakt tussen verschillende categorieën gegevens al naar gelang de mate van nauwkeurigheid en betrouwbaarheid (art. 6(1) Richtlijnvoorstel);
- de eis dat persoonsgegevens 'gebaseerd op feiten' worden onderscheiden van persoonsgegevens 'gebaseerd op persoonlijke beoordelingen' (art. 6(2) Richtlijnvoorstel).

[64] Proposal for a Directive, on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.1.2012, COM(2012) 10final, http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf (geraadpleegd 1 maart 2012).

Deze laatste drie eisen zijn interessante bepalingen die meegenomen zouden kunnen worden in het ontwerp van iColumbo, in aanvulling op de reeds bestaande verplichtingen om gegevens bepaalde markeringen mee te geven.

4.1.7. Conclusie

Hoewel men geneigd kan zijn om het algemene art. 2 Politiewet 1993 als een toereikende grondslag te zien voor politieel openbrononderzoek, valt – vanwege het gebruik van technische hulpmiddelen en de intensiteit van het zoeken in uiteenlopende Internetbronnen – te betogen dat gebruik van iColumbo snel als stelselmatige observatie aan te merken is. Wanneer het gebruik van iColumbo een uitgebreidere zoekactie betreft, maakt dit een meer dan geringe inbreuk op de privacy en is dit alleen mogelijk in het kader van de opsporing; uitgebreidere zoekacties zijn niet mogelijk in het kader van de algemene politietaak, zoals in het algemeen 'surveilleren op Internet'. Voor uitgebreidere zoekacties dient de opsporingsambtenaar een bevel van de officier van justitie ex art. 126g Sv te vragen. Wanneer men bij openbrononderzoek de identiteit (zoals het IP-adres) afschermt, is er bovendien mogelijk sprake van misleiding, waardoor mogelijk een bevel van de officier tot stelselmatig inwinnen van informatie (art. 126j Sv) nodig is. Dit geldt a fortiori voor onderzoek van gegevens in semi-open bronnen waarvoor registratie nodig is, bijvoorbeeld wanneer een opsporingsambtenaar een Hyves- of Facebookprofiel aanmaakt onder pseudoniem.

Een en ander betekent dus dat verdergaand openbrononderzoek niet mogelijk is in het kader van handhaving van de openbare orde maar alleen kan worden ingezet voor opsporing. Daarbij is in beginsel een keuringsrapport nodig dat aangeeft dat iColumbo voldoet aan de eisen van het Besluit technische hulpmiddelen; aangezien de eisen daarvan meer toegespitst zijn op fysieke hulpmiddelen en niet op programmatuur, moet nader onderzocht worden hoe het best de functionele eisen van het Besluit (zoals niet-manipuleerbaarheid van resultaten) kunnen worden toegepast en getoetst voor iRN/iColumbo; het onderzoek van de Radboud Universiteit zal hier naar verwachting goede aanknopingspunten voor bieden. Voorts moet de politie zeer terughoudend zijn met het geautomatiseerd verzamelen en verwerken van fotomateriaal uit open bronnen, aangezien dit gevoelige persoonsgegevens zijn die alleen mogen worden verwerkt als dit onvermijdelijk is voor het doel van het onderzoek.

Ervan uitgaand dat de opslag van iColumbo-zoekacties dusdanig gebeurt dat het een gestructureerd geheel betreft waarop verdere zoekacties en bewerkingen mogelijk zijn, is de Wet politiegegevens van toepassing op deze gegevensverzameling. De verwerking is dan gebonden aan diverse wettelijke eisen betreffende nauwkeurigheid, relevantie, doelbinding en bewaartermijnen (die verschillen afhankelijk van het kader waarbinnen de politiegegevens zijn verzameld). Nadat gegevens volgens de wettelijke plichten zijn verwijderd, moeten ze nog vijf jaar apart bewaard worden voor controledoeleinden. Voor vergelijking van gegevens binnen iColumbo of van iColumbo-gegevens met andere geregistreerde politiegegevens, is een specifieke autorisatie van de opsporingsambtenaar nodig. Ook moeten gegevens kunnen worden gemarkeerd en zo nodig afgeschermd. De reikwijdte van de inzagerechten van betrokken in iColumbo vergt nader onderzoek; in elk geval moet een technische mogelijkheid bestaan om inzage te krijgen en om gegevens te corrigeren, verwijderen of af te schermen.

4.2. Belastingdienst

4.2.1. Inleiding

De Belastingdienst kent drie verschillende soorten gebruikers van het iRN/iColumbo. In de eerste plaats de 'Belastingdienst Blauw'. Hieronder vallen alle heffingen en toelages. De Belastingdienst Blauw is van oorsprong vooral reactief ingesteld. De burger of het bedrijf moet een aangifte invullen, waarop de Belastingdienst reageert. Een meer recente doelstelling richt zich op meer preventieve actie, wat inhoudt dat de Belastingdienst Blauw, onder andere via Internet, een indruk wil krijgen van de behoeften die spelen in de markt, om zo proactief, bijvoorbeeld door gerichte reclame aan burgers en bedrijven, nadere informatie te verschaffen over de producten en diensten van de Belastingdienst. In de tweede plaats vormt de Douane een onderdeel van de Belastingdienst dat gebruik zal maken van iRN/iColumbo. De Douane is verantwoordelijk voor de goederen die de Nederlandse grenzen overgaan en zal in dit kader zogenaamde 'background checks' willen doen op bedrijven en eventueel personen, om te zien of een bepaalde zending te

vertrouwen is. Het is relevant erop te wijzen dat de Koninklijke Marechaussee een andere organisatie betreft dan de Douane. Dit met het oog op artikel 6 van de Politiewet, waarin de Koninklijke Marechaussee expliciet bepaalde politietaken krijgt opgedragen, terwijl de vraag of de Douane persoonsgegevens verwerkt in het kader van de uitoefening van de Politietaak minder eenvoudig te beantwoorden is. In de derde plaats heeft de Belastingdienst een eigen opsporingsdienst, de FIOD-ECD (Fiscale Inlichtingen- en Opsporingsdienst / Economische Controle Dienst). Sinds 2003 hoort ook de opsporingstak van Buma/Stemra bij deze organisatie. Het doel van deze groep binnen de Belastingdienst is het leveren van een bijdrage aan het strafrechtelijk tegengaan van fiscale, financiële en economische fraude; het waarborgen van een integer beroeps- en bedrijfsleven; en de bestrijding van de georganiseerde criminaliteit.[65]

In het kader van opsporingsonderzoek zal iRN/iColumbo gebruikt worden voor gericht onderzoek naar één enkele persoon. Hierbij wordt niet uitgesloten dat gebruik gemaakt zal worden van bijzondere opsporingsmethoden zoals infiltratie en pseudokoop. Wettelijk zijn deze bevoegdheden voorbehouden aan (bijzondere) opsporingsdiensten en zullen deze methoden dus enkel ingezet kunnen worden door personen of diensten aan wie binnen de Belastingdienst bij wet dergelijke bevoegdheden zijn toegekend. Het gebruik dat gemaakt zal worden van iRN/iColumbo verschilt dus met name tussen enerzijds de Belastingdienst Blauw en anderzijds de Douane en de FIOD-ECD. Bij de eerste dienst zal het om het vaststellen van een globaal beeld gaan, terwijl het gebruik zich bij de laatste twee specifiek zal (kunnen) richten op personen. Het gebruik bij de Douane en de FIOD-ECD zal daarom mogelijk meer privacygevoelig zijn dan bij de Belastingdienst Blauw. Niet alleen het type gebruik, maar ook het doel waarvoor gegevens verwerkt worden in het kader van iRN/iColumbo verschilt bij de drie diensten, en ook de wettelijke grondslagen voor de verwerking van persoonsgegevens kunnen per dienst verschillen. De Belastingdienst biedt daarom een goed voorbeeld waarom niet organisatiebreed uitspraken gedaan kunnen worden over de rechtmatigheid van gegevensverwerking met behulp van iRN/iColumbo. Per gegevensverwerking moet gekeken worden of voldaan wordt aan de wettelijke vereisten die voortvloeien uit de Wbp of de Wet politiegegevens.

Aangezien de Belastingdienst als zodanig valt binnen de reikwijdte van de Wbp, zijn alle in paragraaf 2.3 besproken randvoorwaarden met betrekking tot eerlijke en rechtmatige verwerking van persoonsgegevens van toepassing op alle drie de diensten van de Belastingdienst. Echter, wanneer de Belastingdienst gegevens verwerkt in het kader van de uitoefening van de politietaak, waarvan sprake zal zijn bij opsporing, is niet de Wbp maar de Wet politiegegevens van toepassing (par. 4.1.5). Zoals eerder aangegeven kan verder binnen de toepasselijkheid van één regime bovendien sprake zijn van verschillende grondslagen en daarmee bevoegdheden op basis waarvan persoonsgegevens en/of gevoelige gegevens al dan niet verwerkt mogen worden. Hieronder wordt eerst kort stilgestaan bij de algemene bevoegdheden die met betrekking tot de Belastingdienst verankerd liggen in de Algemene wet inzake rijksbelastingen (AWR). Daarna wordt meer specifiek voor de Douane en de FIOD-ECD gekeken naar bijzondere bevoegdheden.

Naast de drie officiële rollen van de Belastingdienst, geldt bovendien in het kader van iRN/iColumbo nog een vierde rol, namelijk als medeontwikkelaar. De Belastingdienst levert ook onderdelen voor het iColumbo-systeem. Hierdoor is de Belastingdienst ook een toeleverancier van iColumbo. In deze rol test de Belastingdienst het iColumbo-systeem. Juist in deze rol als medeontwikkelaar kan het probleem dat eerder beschreven is ten aanzien van het verbod om gevoelige gegevens te mogen verwerken (par. 2.3.3, tweede laag) een rol spelen. De variant die in dit kader beschreven wordt om voor de tests met echte data het systeem mee te laten draaien in een bestaand onderzoek, lijkt een goede optie. Het bestaande onderzoek loopt dan zelfstandig, maar het systeem laat men ernaast lopen om te zien hoe dit functioneert.

4.2.2. Algemene bevoegdheden

De taken en bevoegdheden van de Belastingdienst zijn voor een groot deel verankerd in de Algemene wet inzake rijksbelastingen (AWR). In hoofdstuk VIII 'Bijzondere bepalingen' staat een aantal artikelen opgenomen die de vergaring van gegevens betreffen (zie met name art. 47 en 52). Het gaat hierbij om plichten voor een ieder om desgevraagd aan de inspecteur gegevens te verstrekken, waarbij ook gegevens die zich bij een derde bevinden door deze derde op verzoek verstrekt moeten worden. Hierbij kan geen beroep worden gedaan op geheimhoudingsplichten.

[65] Brochure *FIOD – ECDP De opsporingsdienst van de belastingdienst,* beschikbaar via: http://download.belastingdienst.nl/belastingdienst/docs/corporate_brochure_fiod_ecd_fi0501z3edned.pdf.

Alleen beklederS van een geestelijk ambt, notarissen, advocaten, artsen en apothekers kunnen zich, met betrekking tot een weigering om te voldoen aan de verplichtingen ten behoeve van de belastingheffing van derden, beroepen op de professionele ambtsgeheim. Deze bevoegdheden zeggen echter niets over de bevoegdheid voor de Belastingdienst om actief informatie te vergaren vanuit open bronnen op Internet. Zoals eerder beschreven vereist artikel 8 lid 2 EVRM dat wanneer sprake is van inbreuken op de privacy, deze voorzienbaar moeten zijn bij wet (zie par. 2.2.2). Voor zover er geen sprake is van verwerkingen ten behoeve van de politietaak (die gefundeerd kunnen worden op artikel 2 Politiewet of een opsporingsbevoegdheid, vgl. par. 4.1), moet worden teruggevallen op een extensieve uitleg van de bepalingen 47 en 52 AWR, of meer in het algemeen op de AWR als geheel. In de AWR staan de taken en bevoegdheden van de Belastingdienst beschreven, op basis waarvan het, in ieder geval tot op zekere hoogte, voorzienbaar is voor burgers dat de Belastingdienst bij de uitoefening van deze taken gebruik zal maken van haar ter beschikking staande informatie.

Gezien het bovenstaande, en vanuit het perspectief van de Wbp (zie par. 2.3.3), zal de Belastingdienst Blauw zich niet kunnen beroepen op een wettelijk plicht als legitieme verwerkingsgrond (artikel 8 onder c Wbp). Ook lijkt artikel 8 onder e Wbp niet toepasbaar; het zal immers niet eenvoudig zijn aan te tonen dat het voor de goede vervulling van een publiekrechtelijke taak *noodzakelijk* is persoonsgegevens uit open bronnen te verwerken. Daarom blijft over artikel 8 onder f (belangenafweging), waarin noodzakelijkheid ook een rol speelt. Gegevens mogen op basis van deze grondslag alleen verwerkt worden indien dit noodzakelijk is ter behartiging van het gerechtvaardigde belang van de verantwoordelijke (of van een derde aan wie de gegevens worden verstrekt), tenzij het privacybelang van de betrokkene zwaarder weegt. Het criterium van noodzakelijkheid vereist ook vanuit het perspectief van artikel 8 EVRM de nodige onderbouwing, aangezien inbreuken op de privacy enkel zijn toegestaan voor zover zij noodzakelijk zijn in een democratische samenleving. Met betrekking tot de wijze waarop Belastingdienst Blauw gebruik maakt van iRN/iColumbo, kan gesteld worden dat de privacyinbreuken niet erg diepgaand zijn; meestal zal niet specifiek op individuen worden ingezoomd, en ook speelt een rol dat informatie uit open bronnen afkomstig is. Dit gebruik kan in dat licht proportioneel worden geacht, waarbij artikel 8 onder f als grondslag kan gelden. Dat vereist niettemin wel dat verder alle rechten en verplichtingen uit de Wbp correct worden nageleefd, in het bijzonder de vereisten van dataminimalisatie, doelbinding en het (tijdig) verwijderen of anonimiseren van gegevens. Immers, met het oog op het doel van het gebruik van iRN/iColumbo bij Belastingdienst Blauw – het verkrijgen van een algemeen beeld van de markt – lijkt het niet noodzakelijk om persoonsgegevens, ofwel gegevens die een natuurlijk persoon identificeren, te bewaren. Dergelijke gegevens zullen dan ook zo spoedig mogelijk (onomkeerbaar) moeten worden geanonimiseerd of verwijderd.

Bij bespreking van Belastingdienst Blauw zijn we ervan uitgegaan dat hier geen sprake is van ambtenaren met een bijzondere juridische positie op het gebied van opsporingstaken. Dit is echter wel mogelijk, aangezien bij besluit voor de Belastingdienst is vastgelegd dat zijn aangewezen als buitengewoon opsporingsambtenaar ‘de personen werkzaam in de functie van verbalisant of fraudecoördinator in dienst bij de Belastingdienst’.[66] Op grond van het vierde artikel van dit Besluit is de buitengewoon opsporingsambtenaar bevoegd tot het opsporen van de strafbare feiten behorend tot het domein ‘Werk, Inkomen en Zorg’, van bijlage A-I van de Circulaire Buitengewoon opsporingsambtenaar, voor zover noodzakelijk voor een goede vervulling van de aan deze functie gerelateerde taken. Van belang is nog dat het tweede lid bepaalt dat de opsporingsbevoegdheid, bedoeld in het eerste lid, geldt voor het grondgebied van Nederland.[67] Zoals hieronder nader uitgelegd wordt in het kader van de Douane kan er bij dit type ambtenaren, en voor zover zij gegevens verwerken binnen de reikwijdte van de hierboven beschreven taakstelling, sprake zijn van toepasselijkheid van de Wet politiegegevens in plaats van de Wbp.

[66] Besluit van de Staatssecretaris van Veiligheid en Justitie van 9 december 2010, nr. 5675480/Justis/10, strekkende tot aanwijzing van buitengewoon opsporingsambtenaren bij de Belastingdienst, artikel 2.

[67] Ook artikel 146 WvSv bepaalt dat de bevoegdheid van ambtenaren met de opsporing van strafbare feiten belast, is beperkt tot het grondgebied waarvoor zij zijn aangesteld of waar zij in overeenstemming met de bepalingen van de Politiewet 1993 buiten dat grondgebied hun taak vervullen. Dit type bepalingen zijn potentieel problematisch voor openbrononderzoek waarbij het overschrijden van de landsgrenzen een vrijwel onoverkomelijk neveneffect zal zijn. In het kader van opsporing bestaat hiervoor echter wel een verdragsrechtelijke basis; zie hierover par. 4.1.4.

4.2.3. Bijzondere bevoegdheden Douane

Op grond van de handhavingsvisie 2008-2013 van de Douane heeft de Douane de volgende missie: 'De Douane is de handhavingsdienst die de veiligheid, de integriteit en de fiscaliteit van het buitengrensoverschrijdend goederenverkeer controleert en bevordert'.[68] Om deze missie te volbrengen gelden voor de Douane specifieke bevoegdheden die zijn vastgelegd in de Algemene Douanewet (ADW).[69] In deze wet zijn de bevoegdheden van de Douane samengebracht. De ADW bevat naast controle- en toezichtbevoegdheden ook fiscale opsporingsbevoegdheden. Niet-fiscale opsporingsbevoegdheden zijn niet opgenomen in de ADW maar kunnen wel voortvloeien uit specifieke wetgeving waarin de Douane is aangewezen als opsporingsbevoegd of uit het Besluit buitengewoon opsporingsambtenaar Belastingdienst/Douane.[70] Voor de controlebevoegdheden geldt bovendien dat deze integraal zijn opgenomen in de ADW; er is dus niet volstaan met een verwijzing naar de Algemene wet bestuursrecht.

Alvorens in te gaan op de specifieke bevoegdheden die vermeld staan in de artikelen 1.23 e.v. ADW, wordt eerst kort gewezen op de artikelen 1.20 en 1.21 die invulling geven aan enkele algemene beginselen van behoorlijk bestuur. Het gaat hier om de bepaling dat bevoegdheden enkel aangewend mogen worden voor douanetoezicht en -controle ingevolge het bepaalde bij en krachtens de ADW (Art. 1.20). Daarnaast geldt voor de Douane op grond van artikel 1.21 ADW dat slechts van de bevoegdheden gebruik gemaakt mag worden voor zover dit redelijkerwijs voor de vervulling van zijn taak nodig is. Ook het beginsel van subsidiariteit is in dit artikel neergelegd: van de bevoegdheden die de inspecteur ter beschikking staan moet het minst ingrijpende middel gekozen worden.

Hoewel slechts enkele van de hieronder te noemen bevoegdheden van de inspecteurs van de Douane relevant lijken met het oog op onderzoek in open bronnen, worden toch kort alle bevoegdheden aangehaald. De reden hiervoor is om te illustreren dat deze bevoegdheden verstrekkend zijn, en zwaar kunnen ingrijpen in de persoonlijke levenssfeer. Deze inbreuk is vaak zwaarder dan onderzoek in open bronnen, waarvoor niet expliciet een bevoegdheid is opgenomen. Dit roept, mede vanuit het oogpunt van subsidiariteit, de vraag op of geredeneerd kan worden dat gezien de expliciete toekenning van meer ingrijpende bevoegdheden, het inzetten van een minder ingrijpend middel, het zoeken in open bronnen, toelaatbaar kan worden geacht, ook als dat niet expliciet wordt benoemd.

Op grond van de ADW hebben inspecteurs van de Douane de volgende bevoegdheden:

1. met medeneming van de benodigde apparatuur of dieren elke plaats te betreden (art. 1.23);[71]
2. onderzoek van goederen en het eventueel nemen van monsters voor analyse of grondige controle ingeval geen aanvaarding van een douaneaangifte heeft plaatsgevonden (art. 1.24);
3. onderzoek van een groep of partij goederen of de controle achteraf van de aangiften kan geschieden door middel van een gedeeltelijk onderzoek (art. 1.25);
4. gebouwen niet zijnde woningen en bepaalde terreinen en vervoermiddelen te onderzoeken (art. 1.26);
5. vervoermiddelen vaart te doen minderen of te laten stilhouden (art. 1.27) of in beslag nemen (art. 1.37);
6. lijfvisitatie (art. 1.28);
7. aanbrengen van versperringen op openbare land- en waterwegen (art. 1.29);
8. gebruik van geweld (art. 1.30);
9. opleggen van een dwangsom (art. 1.31).

De artikelen 1.32 en 1.33 betreffen gegevens en inlichtingen. In artikel 1.32 gaat het om het verkrijgen van gegevens, terwijl het in artikel 1.33 gaat om het uitwisselen van gegevens tussen verschillende overheidsdiensten en douaneautoriteiten van andere lidstaten. Vanuit het oogpunt van een legitieme verwerkingsgrond in het kader van de Wbp voor onderzoek in open bronnen komt artikel 1:32 ADW het meest in de richting. Dit artikel bepaalt dat het toegelaten moet worden dat kopieën, leesbare afdrukken of uittreksels worden gemaakt van de voor raadpleging beschikbaar gestelde gegevensdragers of de inhoud daarvan. Mogelijk kan het gebruik van iRN/iColumbo op dit artikel worden gebaseerd. Het is echter de vraag of materiaal in open

[68] Ministerie van Financiën (2008, 22 juli). Rechtshandhaving door de Douane 2008–2013.
[69] Voor een verhandeling over de verschillen tussen de oude Douanewet en de nieuwe Algemene Douanewet zie Janssen 2009.
[70] Besluit van de Minister van Justitie d.d. 26 november 2007, nr. 5518463/07. Dit Besluit vervalt op 1-12-2012.
[71] Hij kan zich doen vergezellen van personen die daartoe door hem zijn aangewezen, Art. 1.23, lid 2.

Internetbronnen kan worden beschouwd als 'voor raadpleging [door de Douane] beschikbaar gesteld'. Het ligt misschien meer voor de hand om, zoals hierboven bij Belastingdienst Blauw beschreven, de voorzienbaarheid bij wet te baseren op het geheel aan taken en bevoegdheden dat voortvloeit uit de ADW, op basis waarvan burgers zouden kunnen voorzien dat de Douane ook gebruik zal maken van openbaar beschikbare bronnen zoals het Internet.

Naast de Algemene Douanewet is het nodig een blik te werpen op het Besluit buitengewoon opsporingsambtenaar Belastingdienst/Douane 2007. Dit met name om vast te stellen of op de verwerking van persoonsgegevens door de Douane de Wbp van toepassing is of de Wet politiegegevens. Uit artikel 2 Politiewet 1993 volgt dat de politie tot taak heeft de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Op grond van artikel 3 zijn ambtenaren van politie in de zin van deze wet onder andere die ambtenaren die zijn aangesteld voor de uitvoering van de politietaak. In het Besluit buitengewoon opsporingsambtenaar Belastingdienst/Douane 2007 wordt voor een specifiek gebied een opsporingsbevoegdheid toegekend aan zogenaamde buitengewoon opsporingsambtenaren.[72] Als dergelijke ambtenaren worden aangemerkt diegenen die hiertoe zijn beëdigd en werkzaam zijn als ambtenaren belast met surveillance- of opsporingstaken. Voor deze personen geldt aldus dat zij, voor het specifieke gebied waartoe zij als bevoegd zijn aangewezen, de verwerking van persoonsgegevens handelen in de uitvoering van de politietaak, immers het handhaven van de rechtsorde. Voor deze verwerkingen geldt niet het regime van de Wbp maar dat van de Wet politiegegevens. Voor alle andere ambtenaren werkzaam bij de Douane, of voor die verwerkingen die niet geschieden ten behoeve van de uitvoering van de politietaak, geldt in beginsel wel de Wbp.

Zoals opgemerkt in par. 4.1.1 geldt voor de politie geen specifieke bevoegdheid voor openbrononderzoek. Ook voor de Douane geldt dat een dergelijke specifieke bevoegdheid niet bestaat en dus moet worden teruggevallen op artikel 2 Politiewet 1993, met alle beperkingen van dien (zie par. 4.1.1).

Belangrijke verschillen die vanuit een oogpunt van openbrononderzoek bestaan tussen de Wbp en de Wet politiegegevens zijn met name een iets ruimere mogelijkheid om gevoelige gegevens te verwerken op grond van de Wet politiegegevens. Artikel 5 bepaalt in dit verband dat de verwerking van politiegegevens[73] betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en *voor zover dit voor het doel van de verwerking onvermijdelijk is*. Deze bepaling biedt mogelijk enige ruimte ten opzichte van het eerder geconstateerde probleem dat met het zoeken in open bronnen haast onvermijdelijk gevoelige gegevens worden verwerkt, terwijl in de Wbp hiervoor als uitgangspunt een verbod geldt. Een tweede belangrijk verschil, of wellicht beter nadere uitwerking van de beveiligingsplicht, is artikel 6 Wet politiegegevens betreffende autorisaties. Zeker in het kader van de Belastingdienst, waar binnen een organisatie verschillende divisies met verschillende juridische status en bevoegdheden ressorteren, en bovendien binnen elke divisie ambtenaren met een verschillende juridische pet op kunnen werken, is het van groot belang dat een deugdelijke invulling gegeven wordt aan het vereiste dat de verantwoordelijke een systeem van autorisaties onderhoudt dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Een dergelijk systeem van autorisaties moet bij de ontwikkeling van iRN/iColumbo aldus voorzien en geïmplementeerd worden.

4.2.4. Bijzondere bevoegdheden FIOD-ECD

Voor de FIOD-ECD geldt weer een ander regime. Op grond van artikel 141 onder d Wetboek van Strafvordering geldt dat met de opsporing van strafbare feiten zijn belast 'de opsporingsambtenaren van de bijzondere opsporingsdiensten, bedoeld in artikel 2 van de Wet op de bijzondere opsporingsdiensten'. De FIOD-ECD valt onder artikel 2, aanhef en onder a van deze wet: een bijzondere opsporingsdienst, ressorterend onder Onze Minister van Financiën. Uit

[72] Voor het opsporen van de strafbare feiten genoemd in domein VI 'Generieke Opsporing', van bijlage A-I van de Circulaire Buitengewoon opsporingsambtenaar, voor zover noodzakelijk voor een goede vervulling van de aan de functie gerelateerde taken. Zie art. 2 Besluit buitengewoon opsporingsambtenaar Belastingdienst/Douane 2007.
[73] Elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (art. 1 onder a Wet politiegegevens).

het tweede hoofdstuk van de Wet op de bijzondere opsporingsdiensten blijkt dat het takenpakket van dergelijke bijzondere opsporingsdiensten de strafrechtelijke handhaving van de rechtsorde betreft op de beleidsterreinen waarvoor de betrokken Minister verantwoordelijkheid draagt. Ook hier is dus sprake van de daadwerkelijke handhaving van de rechtsorde en dus van het mede uitvoering geven aan de politietaak.

Naast de algemene regeling in de Wet op de bijzondere opsporingsdiensten geldt voor de SIOD en FIOD-ECD nog een andere regeling[74] Op grond van deze regeling heeft de Belastingdienst/FIOD-ECD mede tot taak het opsporen van strafbare feiten op het terrein van de arbeidsmarkt voor zover gepleegd in samenhang met strafbare feiten op het terrein van de loonbelasting, premies voor de werknemersverzekeringen of de premie voor de volksverzekeringen en voor zover eerstbedoelde strafbare feiten niet zijn te beschouwen als het hoofdbestanddeel van het complex van geconstateerde strafbare feiten.

Met betrekking tot de verwerking van persoonsgegevens is voorts relevant het Besluit politiegegevens bijzondere opsporingsdiensten.[75] Artikel 1 bepaalt dat voor de FIOD-ECD de verantwoordelijke de Minister van Financiën is. Artikel 2 luidt:

> 1. Onverminderd artikel 46, eerste lid, van Wet politiegegevens is het bij die wet bepaalde met betrekking tot de verwerking van politiegegevens van overeenkomstige toepassing op de verwerking van persoonsgegevens door de bijzondere opsporingsdiensten, met uitzondering van artikel 10, eerste lid, de onderdelen b en c, derde lid en vierde lid, artikel 16, eerste lid, onderdeel d, en de artikelen 37 tot en met 45.
>
> 2. Onverminderd artikel 46, eerste lid, van de wet is het in het Besluit politiegegevens bepaalde met betrekking tot de verwerking van politiegegevens van overeenkomstige toepassing op de verwerking van persoonsgegevens door de bijzondere opsporingsdiensten, met uitzondering van de artikelen 2:4, 2:5, tweede lid, 2:7, 2:13, tweede lid, 3:2, 4:1, eerste lid, onderdeel b, en tweede lid, 4:2, eerste lid, de onderdelen a, c, d, e, f, i, j, k, o en q, en 6:6 van het Besluit politiegegevens.

Hoewel de Minister van Financiën op papier de verantwoordelijke voor de verwerking van politiegegevens door de Belastingdienst/FIOD-ECD is, heeft hij voor de bevoegdheden die uit de Wet politiegegevens voor hem voortvloeien mandaat verleend aan de voorzitter van het managementteam van de Belastingdienst/FIOD-ECD. Dit is vastgelegd in het Mandaatbesluit Wet politiegegevens FIOD-ECD. Het besluit betreft niet enkel het uitoefenen van de bevoegdheden die uit de Wet politiegegevens voortvloeien, maar ook die voortvloeien uit het Besluit politiegegevens en het Besluit politiegegevens bijzondere opsporingsdiensten. De Minister verleent mandaat aan de overige leden van het managementteam van de FIOD-ECD om bij ontstentenis van de voorzitter alle hem toekomende bevoegdheden uit de genoemde wetgeving uit te kunnen oefenen. Ook is bepaald dat de gemandateerde ondermandaat kan verlenen voor met name te noemen bevoegdheden aan medewerkers van de FIOD-ECD, voor zover deze de aan betrokkene opgedragen taak rechtstreeks aangaat. Hierbij is het van belang erop te wijzen dat enkele uitzonderingen gelden met betrekking tot ondermandaat, waaronder toegang tot politiegegevens door een bewerker die niet rechtstreeks onder het gezag van de gemandateerde is onderworpen, het aanwijzen van de functionaris die is belast met het effectueren van besluiten met betrekking tot het autoriseren van medewerkers in een geautomatiseerde omgeving en het vernietigen van gegevens.[76]

4.2.5. Conclusie

Voor de Belastingdienst geldt een divers palet aan taken en bevoegdheden. Hierdoor valt het gebruik van iRN/iColumbo binnen de Belastingdienst onder verschillende regelingen. Bovendien kunnen verschillende personen of diensten verantwoordelijk zijn voor de verwerking van persoonsgegevens. De in een van de interviews geopperde gedachte dat het systeem de verantwoordelijke is omdat bij voorbaat het systeem zelfstandig data verzamelt, gaat niet op; de

[74] Regeling van de Staatssecretaris van Sociale Zaken en Werkgelegenheid en de Staatssecretaris van Financiën van 4 september 2007, nr. SIOD/07/4362, tot toedeling van bepaalde opsporingstaken aan de Sociale Inlichtingen- en Opsporingsdienst en de Belastingdienst/Fiscale Inlichtingen- en Opsporingsdienst en Economische Controledienst (Regeling toedeling bepaalde opsporingstaken SIOD en FIOD-ECD).

[75] Besluit van 3 juli 2009, houdende bepalingen inzake de overeenkomstige toepassing van de Wet politiegegevens op de verwerking van persoonsgegevens door een dienst van een publiekrechtelijk lichaam die is belast met de opsporing van strafbare feiten (Besluit politiegegevens bijzondere opsporingsdiensten).

[76] Zie voor de volledige uitzondering artikel 3 lid 4 van het Mandaatbesluit Wet politiegegevens FIOD-ECD.

verantwoordelijke is degene die het gebruik van het middel (iRN/iColumbo) aanwijst en de doelen bepaalt van het concrete gebruik daarvan. Dat zal dus voor de drie onderscheiden diensten verschillen.

Voor zover het systeem gebruikt wordt in het kader van de uitoefening van de politietaak, gelden dezelfde voorwaarden en beperkingen zoals besproken in hoofdstuk 4.1. Hierbij kan bijvoorbeeld gewezen worden op de conclusie dat bij surveilleren op Internet terughoudend gebruik moet worden gemaakt van iRN/iColumbo om gegevens over specifieke personen uit verschillende bronnen te verzamelen en geautomatiseerd te combineren. Een ander punt betreft de maskering van IP-afkomst, waarvoor tot het moment dat de wetgever zich hierover uitspreekt, het raadzaam is om hiervoor een bevel van de officier vragen.

Voor zover het systeem niet gebruikt wordt met het oog op de uitoefening van de politietaak, geldt vanuit het perspectief van artikel 8 EVRM dat met name aandacht besteed moet worden aan het vereiste van voorzienbaarheid. Deugdelijke informatievoorziening kan bijdragen aan de mogelijkheid om een de algemene taakstelling van de Belastingdienst aan te voeren als wettelijke basis. Ook de noodzakelijkheid in een democratische samenleving behoeft nadere onderbouwing. Bovendien geldt op basis van het wettelijk kader van de Wbp dat strikte randvoorwaarden geschapen moeten worden om de verwerking van gevoelige persoonsgegevens zoveel mogelijk te voorkomen, aangezien geen enkele uitzondering op het verbod gevoelige gegevens te verwerken een sterke basis biedt voor de Belastingdienst om gevoelige gegevens uit open bronnen te verwerken.

4.3. MIVD

4.3.1. Grondslag voor bevoegdheden

Een algemene bevoegdheid tot het verzamelen van gegevens, onder andere uit openbare bronnen, kan worden gelezen in art. 12 lid 1 Wiv 2002:

> De diensten zijn bevoegd tot het verwerken van gegevens met inachtneming van de eisen die daaraan bij of krachtens deze wet of de Wet veiligheidsonderzoeken zijn gesteld.

Er staat echter niet met zoveel woorden in dat de diensten een bevoegdheid hebben om gegevens (zoals uit open bronnen) te verzamelen. Indien deze bepaling niet als bevoegdheidscheppend, maar slechts als bevoegdheidsbeperkend gelezen zou moeten worden, dan zou de MIVD kunnen kijken naar art. 17 Wiv 2002, dat een algemene grondslag biedt voor het inwinnen van gegevens over personen bij derden:

> 1. De diensten zijn bevoegd zich bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, voor het verzamelen van gegevens te wenden tot:
>
> a. bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken;
>
> b. de verantwoordelijke voor een gegevensverwerking.

De bepaling van art. 17 lid 1 Wiv 2002 past echter minder goed bij openbrononderzoek, omdat zij uitgaat van een derde bij wie de gegevens ingewonnen worden en dat is allicht iets anders dan het eenzijdig verzamelen van gegevens die in openbare bronnen voor het oprapen liggen. Enige steun voor de opvatting dat art. 17 Wiv 2002 geen grondslag biedt voor het verzamelen van gegevens uit openbare bronnen biedt ook de Memorie van Toelichting. Sprekend over art. 12 noemt de toelichting de open bronnen nevenschikkend aan de raadpleging van personen als bedoeld in art. 17 Wiv 2002:

> Bij de verwerking van gegevens door de diensten, in het bijzonder de verzameling van gegevens, staan diverse mogelijkheden ter beschikking. Gegevens worden verzameld door kennisneming van voor een ieder toegankelijke bronnen («open bronnen informatie»), door de raadpleging van niet-openbare gegevensverzamelingen, waarvoor de diensten zijn geautoriseerd (zoals bijvoorbeeld de Gemeentelijke basisadministratie persoonsgegevens en de politieregisters), door de raadpleging van personen en instanties die mogelijkerwijs beschikken over voor een dienst relevante gegevens, maar

ook door de uitoefening van de bijzondere bevoegdheden als bedoeld in paragraaf 3.2.2 van het wetsvoorstel.[77]

De keuze van art. 17 Wiv 2002 als grondslag zou bovendien aanleiding geven tot lastige praktische vragen. Bij het verzamelen van gegevens uit openbare Internetbronnen is bijvoorbeeld niet duidelijk tot wie een MIVD-medewerker zich 'formeel' wendt: is dat degene die de gegevens online heeft gezet of is dat de hosting- of platformaanbieder? Is dat voor alle Internetdiensten – bijvoorbeeld het www-pagina's, Usenet of sociale netwerkpagina's – gelijk, of kan de MIVD-medewerker kiezen? Het antwoord op die vraag is relevant in verband met de vraag of de ambtenaar van de MIVD zich als zodanig bekend moet maken bij het opvragen van de gegevens. Het tweede lid van art. 17 Wiv 2002 zegt daarover:

2. In het geval, bedoeld in het eerste lid, aanhef en onder b, is de daarmee belaste ambtenaar verplicht zich ten opzichte van de verantwoordelijke voor een gegevensverwerking te legitimeren aan de hand van een daartoe door het betrokken hoofd van een dienst verstrekt legitimatiebewijs.

Uit het feit dat de legitimatieplicht uitdrukkelijk alleen geregeld is voor het geval de ambtenaar zich wendt tot de verantwoordelijke voor een gegevensverwerking, valt af te leiden dat in andere gevallen de legitimatieplicht niet geldt. In veel gevallen zal de inhoudsaanbieder echter ook verantwoordelijke zijn,[78] zodat de legitimatieplicht dan zou gelden. Maar de ratio van deze legitimatieplicht past slecht in de context van open bronnen. Blijkens de Memorie van Toelichting is de 'ratio voor deze legitimatieplicht (…) daarin gelegen, dat een houder van een verzameling van persoonsgegevens alvorens in te gaan op het verzoek om gegevensverstrekking zich moet kunnen vergewissen dat het verzoek rechtens wordt gedaan door een dienst'.[79] Het gaat er kort gezegd om dat de verantwoordelijke zijn eventuele verstrekking van persoonsgegevens aan de dienst moet kunnen verantwoorden. Gegeven het feit dat de desbetreffende gegevens op Internet staan en niet door een bewuste keuze van de verantwoordelijk al dan niet aan de dienst worden verstrekt, lijkt een legitimatieplicht in dit geval niet daadwerkelijk in een behoefte te voorzien. De beheerder van de gegevens zal zich eerder moeten verantwoorden voor het openbaar maken van de gegevens dan dat hij zich zal moeten verantwoorden voor het feit dat de MIVD de openbare gegevens heeft geraadpleegd.

Al met al ligt het meer voor de hand om art. 12 Wiv 2002 de grondslag te zien voor openbrononderzoek door de MIVD. Het EHRM interpreteert het criterium 'voorzien bij wet' als genoemd in art. 8 lid 2 EVRM ruim (zolang het recht maar voldoende duidelijk en kenbaar is voor burgers) en de bevoegdheid van de MIVD tot het verzamelen van gegevens uit openbare bronnen heeft een zekere vanzelfsprekendheid heeft, zoals ook blijkt uit bovenstaand citaat uit de Memorie van Toelichting. Daarmee is goed te verantwoorden dat de bevoegdheid om uit openbare bronnen (persoons)gegevens te verzamelen op de algemene bepaling van art.12 lid 1 Wiv 2002 is gebaseerd. Art.17 Wiv 2002 kan overigens wel relevant zijn voor vormen van passieve openbaarheid, bijvoorbeeld als iemand openbaar aanbiedt op verzoek per e-mail bepaalde gegevens te zullen toesturen, maar dat zal bij gebruik van iRN/iColumbo veelal niet relevant zijn.

4.3.2. Bijzondere bevoegdheden

Naast haar algemene bevoegdheid heeft de MIVD tevens een aantal bijzondere bevoegdheden die van belang kunnen zijn bij het verzamelen van gegevens uit openbare bronnen. Interessante bevoegdheden zijn de volgende.

- De bevoegdheid, al dan niet met observatie- en registratiemiddelen, personen of zaken te observeren of volgen van art. 20 Wiv 2002. Deze bevoegdheid zou relevant kunnen zijn indien iemands online gedrag stelselmatig gevolgd wordt. Het uitgangspunt is dat stelselmatige observatie een zwaardere inbreuk op privacy oplevert dan een eenmalige zoekactie en derhalve met meer waarborgen omgeven moet zijn. De bepaling lijkt echter meer toegeschreven op een fysieke omgeving (vgl. de discussie in par. 4.1.1).
- Het gebruik van een dekmantel om gericht gegevens te verzamelen over personen en organisaties die voor de taakuitvoering relevant zijn (art. 21 onder a sub 1 Wiv 2002). Deze bevoegdheid zou relevant kunnen zijn bij situaties van passieve openbaarheid, bijvoorbeeld

[77] *Kamerstukken II* 1997/98, 25 877 nr. 3, par. 3.3 .
[78] Zie EHJ, zaak C-101/01, 6.11.2003 (Lindqvist) en Groep gegevensbescherming artikel 29 (2009).
[79] *Kamerstukken II* 1997/98, 25 877 nr. 3, par. 3.4.2.

indien de verwachting bestaat dat de gegevens niet beschikbaar gemaakt zullen worden indien de ware identiteit of hoedanigheid van de vrager bekend is. Deze bepaling zou ook de situatie kunnen dekken waarin bronnen worden geraadpleegd waarvoor registratie nodig is.
- De bevoegdheid tot hacken (art. 24 Wiv 2002). Deze bevoegdheid zou relevant kunnen zijn bij het omzeilen van beveiligingen tegen het uitmelken van een openbare databank.

Artikel 31 Wiv 2002 bepaalt dat dit soort bijzondere bevoegdheden alleen mogen worden ingezet als het doel niet (tijdig) kan worden bereikt 'door raadpleging van voor een ieder toegankelijke informatiebronnen'. Dat impliceert dat de MIVD zich in beginsel moet beperken tot de basisfunctionaliteit van iRN/iColumbo (en dus niet stelselmatig personen moet volgen via het systeem of beveiligingen van databanken tegen uitmelken omzeilen), tenzij het doel van het onderzoek het nodigt maakt om deze meer ingrijpende bevoegdheden in te zetten.

Een belangrijke beperking is dat de bijzondere bevoegdheden alleen voor een beperkt aantal taken mogen worden ingezet (art.18 Wiv 2002), te weten de taken genoemd in art. 7 lid 2 onder a, c en e; kort gezegd betreft het onderzoek naar strijdkrachten van andere mogendheden, onderzoek ter bescherming van de eigen strijdkrachten en onderzoek naar aangewezen andere landen. De bijzondere bevoegdheden mogen dus *niet* ingezet worden voor veiligheidsonderzoeken.

Voor zover de MIVD iRN/iColumbo zou willen gebruiken voor andere doelen dan veiligheidsonderzoeken en daarbij verder wil gaan dan de basisfunctionaliteit van (niet-stelselmatig) zoeken in vrij toegankelijke bronnen, dan is het gebruik hiervan onderworpen aan toestemming van de minister of andere gezagsdragers (art. 19 Wiv 2002). De uitoefening van bijzondere bevoegdheden moet bovendien onmiddellijk gestaakt worden zodra het doel hun inzet niet langer nodig maakt (art. 32 Wiv 2002). Er moet verslag worden opgemaakt van de uitoefening van bijzondere bevoegdheden (art. 33 Wiv 2002).

4.3.3. Eisen aan gebruik van bevoegdheden

De verwerking van gegevens vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 2002 of de Wet veiligheidsonderzoeken (art. 12 lid 2 Wiv 2002). Op basis van art 7 lid 2 onder b Wiv 2002, heeft de MIVD in het belang van de nationale veiligheid onder andere tot taak 'het verrichten van veiligheidsonderzoeken als bedoeld in de Wet veiligheidsonderzoeken'. De Wet veiligheidsonderzoeken bepaalt dat de MIVD veiligheidsonderzoeken instelt voor militaire vertrouwensfuncties (inclusief personen die toegang moeten hebben tot militaire installaties) alvorens een verklaring van geen bezwaar afgeleverd kan worden (art. 7 jo 2 Wvho). Bij dit onderzoek wordt onder andere gelet op

> b. gegevens betreffende deelneming of steunverlening aan activiteiten die de nationale veiligheid kunnen schaden;
>
> c. gegevens betreffende lidmaatschap van of steunverlening aan organisaties die doeleinden nastreven, dan wel ter verwezenlijking van hun doeleinden middelen hanteren, die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde;
>
> d. gegevens betreffende overige persoonlijke gedragingen en omstandigheden, naar aanleiding waarvan betwijfeld mag worden of de betrokkene de uit de vertrouwensfunctie voortvloeiende plichten onder alle omstandigheden getrouwelijk zal volbrengen (art. 7 lid 2 Wvho).

Het ligt voor de hand dat voor het verzamelen van deze gegevens gebruik wordt gemaakt van open bronnen; dergelijk gebruik is allicht noodzakelijk voor een goede uitvoering van deze taak. Daarom mag de MIVD iRN/iColumbo gebruiken voor veiligheidsonderzoeken, mits zij voldoen aan de overige eisen uit de Wiv 2002. Deze eisen zijn vergelijkbaar met eisen uit de Wbp en WPolG, zoals verwerking 'op behoorlijke en zorgvuldige wijze' (art. 12 lid 3 Wiv 2002) en het verbod om gevoelige persoonsgegevens te verwerken; dit laatste mag alleen 'in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is' (art. 13 lid 3 en 4 Wiv 2002). Gezien de gevoeligheid van vertrouwensfuncties, zal de drempel van onvermijdelijkheid hier veelal lager liggen dan bij politie of andere opsporingsdiensten, zodat de MIVD vermoedelijk meer ruimte heeft om gevoelige persoonsgegevens (zoals foto's en video's) te verwerken. Er moeten voorzieningen zijn die de

juistheid en volledigheid van gegevens bevorderen, gegevens moeten goed beveiligd worden en er dient een autorisatiesysteem te zijn voor toegang tot verwerkte gegevens (art. 16 Wiv 2002).

Specifiek wordt ook bepaald dat bij gegevens een 'aanduiding omtrent de mate van betrouwbaarheid' moet worden vermeld, dan wel 'een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend'. De logfunctie van iRN/iColumbo komt tegemoet aan deze eis. Een belangrijke beperking is wel dat in het kader van het veiligheidsonderzoek de verwerking van gegevens 'slechts betrekking [kan] hebben op personen (…) die toestemming hebben verleend voor een veiligheidsonderzoek' (art. 13 lid 2 onder b Wiv 2002). Dit lijkt te impliceren dat bij een veiligheidsonderzoek naar persoon A alleen zoekvragen mogen worden gesteld in het iRN/iColumbo-systeem die A betreffen. Zoekvragen naar personen in de kring van A mogen niet worden versteld. Het zal onvermijdelijk zijn dat bij een zoekvraag naar A ook gegevens over andere personen in beeld komen. Naar de letter van de wet zouden deze gegevens niet mogen worden verwerkt, maar dat zou het veiligheidsonderzoek via open bronnen feitelijk onmogelijk maken. Art. 13 lid 2 onder b moet dan ook gelezen worden als een inspanningsverplichting om zo weinig mogelijk 'bijvangst' over andere personen te krijgen. Dat impliceert dat zoekvragen gericht en beperkt moeten zijn, en dat de eindgebruiker zich moet inspannen om, zodra blijkt dat gegevens over andere personen uit het systeem komen, deze gegevens te verwijderen of pseudonimiseren (vgl. het concept van omkeerbare pseudonimisering in hfd. 6).

4.3.4. Korte blik op de toekomst

Voor zover ons bekend zijn er geen wetsvoorstellen aanhangig met betrekking tot de Wiv 2002 die wijzigingen zouden impliceren in het hierboven beschrevene.

4.3.5. Conclusie

De MIVD beschikt over de bevoegdheid om gegevens uit openbare bronnen te verzamelen. Deze bevoegdheid ligt impliciet besloten in de Wiv 2002 (blijkens de Memorie van Toelichting en art. 31 dat zegt dat bijzondere bevoegdheden alleen mogen worden ingezet als de diensten niet kunnen volstaan met raadpleging van voor een ieder toegankelijke informatiebronnen) en kan eventueel ook worden ingelezen in art. 12 Wiv 2002. Een MIVD-medewerker hoeft zich daarbij niet als zodanig kenbaar te maken en mag dus zijn IP-adres afschermen. Wel is de vraag hoe extensief de MIVD iRN/iColumbo mag gebruiken: vergelijkbaar met de politie speelt namelijk de vraag of het grootschalig of herhaaldelijk verzamelen van gegevens uit open Internetbronnen niet meer dan een geringe inbreuk op de privacy oplevert en dus meer een vorm van stelselmatige observatie (als bedoeld in art. 20 Wiv 2002) zou opleveren dan drempelloos toegestaan openbrononderzoek. Als we de redenering zoals gevolgd bij de politie (zie par. 4.1.1) hier toepassen, zou dit betekenen dat de MIVD slechts beperkt gebruikt mag maken van iRN/iColumbo, tenzij men toestemming heeft van de Minister om art. 20 (observatie) toe te passen. Een relevant verschil is wel, voor zover het gaan om veiligheidsonderzoeken, dat de betrokkene expliciet toestemming heeft gegeven voor het doen van een veiligheidsonderzoek, waardoor de inbreuk op diens privacy minder ingrijpend zal zijn dan bij niets vermoedende burgers of verdachten. Sowieso geldt dat de MIVD bij het doen van veiligheidsonderzoeken geen gebruik mag maken van bijzondere bevoegdheden, en zich dus zal moeten beperken tot het vrij toegestane onderzoek van voor iedereen toegankelijke bronnen. Daarbij gelden verder eisen van doelbinding, zorgvuldigheid bij de verwerking, beveiliging en een inspanningsverplichting om het verwerken van gevoelige persoonsgegevens (waaronder visueel materiaal) tot het minimum noodzakelijke te beperken. Ook moet de bron van de gegevens worden vastgelegd (middels de logfunctie) en moeten zoekvragen beperkt zijn en zo gericht mogelijk op de persoon op wie het veiligheidsonderzoek betrekking heeft. De eindgebruiker moet zich inspannen om, zodra blijkt dat gegevens over andere personen uit het systeem komen, deze gegevens te verwijderen of pseudonimiseren.

5. Wet openbaarheid van bestuur

5.1. Inleiding

Deze paragraaf bespreekt de implicaties van de Wet openbaarheid van bestuur (Wob). Met de inzet van iColumbo en iRN wordt een variëteit aan informatie en kennis gegenereerd. Zo is informatie beschikbaar over het gebruik van het platform, de afnemers van de gegenereerde kennis, de geraadpleegde bronnen, de zoekopdrachten en zelfs de individuele personen die de hulpmiddelen hebben benut. Derden zouden met de Wob in de hand openbaarmaking van deze en andere informatie kunnen afdwingen. Concreet wordt in deze paragraaf aandacht besteed aan de vraag in hoeverre de in het kader van iColumbo en iRN gegenereerde en voorhanden informatie binnen de werkingssfeer van de Wob valt en betrokken partijen er daarom rekening mee hebben te houden dat deze informatie met een beroep op de Wob in de openbaarheid kan komen. Tevens zal aandacht worden besteed aan belangen die zich tegen openbaarheid van de informatie kunnen verzetten, zoals het belang van de bescherming van de persoonlijke levenssfeer en het opsporingsbelang.

Alvorens vast te stellen in hoeverre de Wob van toepassing is, volgt onderstaand eerst een overzicht van de informatie die mogelijk 'Wobbaar' zou kunnen zijn. Derden zouden de Wob in kunnen zetten om:

- inzicht te krijgen in de technologieën en tools die gebruikt worden binnen het platform van iColumbo, inclusief de broncode van de tools en welke algoritmes en parameters worden gehanteerd bij de analyseslag die door iColumbo over de informatie wordt gehaald;
- inzicht te krijgen in de partijen die gebruik maken van iRN/iColumbo. Met een beroep op de Wob zou dat bijvoorbeeld concreet betekenen dat openbaar wordt welke handhavings- en opsporingsinstanties gebruik maken van de systemen. Dat geldt in de toekomst ook voor bijvoorbeeld mogelijke partners in andere landen als het systeem daartoe zou worden uitgebreid;
- inzicht te verwerven in de openbare bronnen die zijn gebruikt. Concreet zou een Wob-verzoek ingediend kunnen worden met de vraag welke Internetbronnen worden benut in het kader van de inzet van de tools en op welk moment bepaalde webpagina's zijn benaderd. Daarbij zou men eventueel kunnen verlangen dat in het overzicht onderscheid wordt gemaakt tussen geraadpleegde bronnen die publiekelijk toegankelijk waren enerzijds en de bronnen die werden benaderd nadat werd ingelogd (met een al dan niet vals account) anderzijds. Een relevante vraag is hier natuurlijk: welk belang prevaleert: openbaarheid of geheimhouding met het oog op het onderzoeksbelang?
- een overzicht te krijgen welke individuen concreet het systeem hebben gebruikt. Het systeem logt alles en daarmee is deze informatie in principe achterhaalbaar;
- nadere details te verkrijgen over kwesties die verband houden met informatievragen: welke informatievraag is door gebruikers voorgelegd en welke informatie is aan individuele gebruikers teruggegeven als antwoord op deze vraag?
- ten slotte informatie die verband houdt met de inzet en het gebruik van iRN/iColumbo, maar waarbij deze informatie niet 'panklaar' beschikbaar is. Alles wordt gelogd, maar er is geen geïntegreerd overzicht van de inzet en het gebruik van de systemen. Wel kan dit worden gegenereerd uit de logbestanden. Een belangrijke vraag is dan of de Wob verlangt dat men een extra slag maakt om uit de logbestanden het overzicht te genereren.

Een belangrijke deelvraag die bij veel bovenstaande vragen aan de orde komt, is of de elektronische bestanden, met name het gegevenspakhuis waarin alle zoekopdrachten en -resultaten worden opgeslagen (zodanig dat je elke zoekactie met resultaten volledig kunt 'terugzien') een document in de zin van de Wob is. Dat geldt ook voor het logbestand, waarin elke zoekactie (datum/tijd, persoon, zoektermen) wordt vastgelegd.

5.2. Bestuursorgaan

De eerste te beantwoorden vraag is of betrokken eindgebruikers zoals politie, Belastingdienst (regulier alsook FIOD-ECD) en MIVD onder het regime van de Wob vallen. Art. 1a Wob regelt dat de wet van toepassing is op bestuursorganen (in de zin van art. 1:1 Awb), waarbij slechts een zeer beperkt aantal overheidsorganen van toepassing is uitgesloten. In ieder geval is duidelijk dat alle drie hiervoor genoemde partijen en bijvoorbeeld ook het Openbaar Ministerie (waarbij de officier van justitie als bestuursorgaan wordt aangemerkt[80]) als bestuursorgaan kwalificeren en bovendien niet van de Wob zijn uitgezonderd.[81] Alhoewel de eindgebruikers van de tools momenteel uitsluitend bestuursorganen zijn, kan hier nog worden vermeld dat in bepaalde situaties ook organisaties buiten de publieke sector onder de Wob vallen. Ingevolge art. 1:1 onder b Awb ziet de wet namelijk ook op instanties 'met enig openbaar gezag bekleed'. Met andere woorden, de wet is ook op privaatrechtelijke organisaties van toepassing voor zover het taken betreft die deze organisaties in het kader van het openbaar gezag uitoefenen; een bekend voorbeeld betreft garagehouders voor zover ze APK-keuringen uitvoeren.

Aangenomen mag derhalve worden dat momenteel de eindgebruikers en de beheerder van iColumbo onder de regeling van de Wob vallen.

5.3. Documenten

Een volgende te beantwoorden vraag betreft dan de werkingssfeer van de Wob. Welke van de eerder opgesomde informatie zou in principe 'Wobbaar' zijn? Art. 3, eerste lid, Wob maakt duidelijk dat de werksfeer van de wet beperkt is tot 'informatie opgenomen in documenten'. Daaruit kan direct worden afgeleid dat informatie die niet is opgenomen in een document buiten de reikwijdte van de Wob valt. Cruciaal is dan de vraag wat exact onder het begrip 'document' verstaan moet worden. Uit art. 1 onder b Wob blijkt dat een document een 'bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat' is. Uit zowel de wetsgeschiedenis als jurisprudentie wordt duidelijk dat 'ander materiaal' een rijk scala aan gegevensdragers en op allerhande wijze digitaal vastgelegde informatie omvat, variërend van informatie die zich in databanken bevindt, video- en geluidsbanden, cd-roms tot 'vermoedelijk zelfs sms-, ping- en twitterberichten'.[82]

Kijkend naar de informatie die met betrekking tot tot iColumbo (potentieel) beschikbaar is, is een aantal kwesties hier van belang. Allereerst: kan een overzicht van geraadpleegde openbare Internetpagina's via de Wob openbaar worden? Relevant is hier een uitspraak van de Afdeling Bestuursrechtspraak van de Raad van State uit 2006 naar aanleiding van het verzoek tot openbaarmaking van websites die waren geraadpleegd in het kader van een politieonderzoek naar Londsdale-jeugd.[83] Het verzoek behelsde het leveren van een overzicht en print zowel van de geraadpleegde Internetpagina's als van de automatisch op de computers opgeslagen loggegevens betreffende de geraadpleegde pagina's. De Afdeling kwam aan een oordeel over deze laatste informatie niet toe, nu het tot de vaststelling kwam dat de desbetreffende webpagina's niet konden worden aangemerkt als een document in de zin van de Wob omdat de sites niet onder het bestuursorgaan 'berusten'. 'Voor het aanmerken van een site als een document als bedoeld in de zin van art. 1 aanhef en onder a Wob is mede van belang het antwoord op de vraag of de site onder het betreffende bestuursorgaan berust. De door de korpsbeheerder geraadpleegde sites, die door derden zijn samengesteld en waarvan ten behoeve van het onderzoek geen informatie is gehaald, zijn niet aan te merken als documenten die onder hen berusten.' Deze formulering betekent dat wanneer een bestuursorgaan wél informatie van een Internetpagina haalt – zoals bij iColumbo/iRN veelal het geval zal zijn – wel degelijk sprake is van een onder een bestuursorgaan berustend document.[84]

---

[80] Daalder 2011, p. 116.

[81] Dat geldt evenzeer voor andere potentiële eindgebruikers, zoals KMAR, RIEC's, CJIB, NFI , DNB, SIOD, AFM, UWV, NVWA, NCTV en NMa.

[82] Daalder 2011, p. 134. Daarbij merkt de auteur op dat het denkbaar is dat de OvJ het primaire besluit op het verzoek tot openbaarmaking neemt en het hogere orgaan (de minister van Veiligheid en Justitie in dit geval) op het bezwaarschrift beslist (p. 117).

[83] ABRvS 16 augustus 2006, AB 2006, 337 m.nt.E.J. Daalder, JB 2006/289 m.nt. G. Overkleeft-Verburg. Zie ook ABRvS 12 oktober 2005, JB 2005/326 m.nt. G. Overkleeft-Verburg.

[84] Zie ook Daalder in zijn noot bij ABRvS 16 augustus 2006.

Relevant is verder de eerder geopperde vraag of informatie die verband houdt met de inzet en het gebruik van iRN/iColumbo, maar waarbij deze informatie niet 'panklaar' beschikbaar is, wel beschikbaar gemaakt zou moeten worden, namelijk door het overzicht met een additionele bewerkingsslag te genereren uit de logbestanden. Eenzelfde vraag kan worden gesteld ten aanzien van de zoekopdrachten en zoekresultaten. In het gegevenspakhuis worden deze opdrachten opgeslagen en wel zodanig dat elke zoekactie met resultaten volledig kan worden 'teruggezien'. Dat geldt ook voor het logbestand, waarin elke zoekactie (datum/tijd, persoon, zoektermen) wordt vastgelegd. Is deze informatie potentieel op te vragen met een beroep op de Wob? Het antwoord valt niet eenduidig te geven, maar duidelijk is wel dat serieus rekening met deze mogelijkheid gehouden moet worden. Uit zowel de literatuur als jurisprudentie valt af te leiden dat de term 'berustend' in de hiervoor gegeven definitie ruim moet worden geïnterpreteerd en wel zodanig dat elektronisch opgeslagen informatie 'berust' onder een bestuursorgaan 'zolang deze met de bestaande programmatuur kan worden aangemaakt'.[85] De Wob omvat mede de verplichting tot het opstellen en genereren van informatie die niet als zodanig beschikbaar is. De ondergrens lijkt in de jurisprudentie te zijn getrokken bij situaties waarin het document alleen kan worden gegenereerd na een bewerkelijke selectie waarmee de nodige kosten, tijd en inzet van menskracht zijn gemoeid. Toegespitst op ICT lijkt dit momenteel te betekenen dat wanneer de verzochte informatie met de inzet van ICT op betrekkelijk eenvoudige wijze valt te genereren, deze informatie beschikbaar gemaakt zou moeten worden. Dat ligt anders als voor het genereren van de informatie een nieuwe applicatie ingekocht of ontwikkeld moet worden of als er externe partijen moeten worden ingehuurd.[86]

Een volgende vraag is in hoeverre voor derden via de Wob inzicht te verkrijgen is in de tools die gebruikt worden binnen het platform van iColumbo, inclusief de broncode van de tools en welke algoritmes en parameters worden gehanteerd bij de analyseslag die door iColumbo over de informatie wordt gehaald. Alhoewel de tools open source zijn, is binnen het programma HDIeF wel de wens geuit deze tools niet breed beschikbaar te maken, wat impliceert dat ze bij voorkeur niet integraal onder het regime van de Wob zouden moeten kunnen vallen. Zoals hiervoor al opgemerkt, heeft het begrip 'document' een ruime werkingssfeer en heeft de wetgever meerdere malen bevestigd dat ook de specificaties van software onder dit begrip vallen.[87] Dit impliceert kortom dat ervan uit moet worden gegaan dat ook de broncode van de tools en welke algoritmes en parameters worden gehanteerd in principe binnen het bereik van de Wob vallen.

Ten slotte is interessant de vraag of het belang van openbaarmaking verlangt dat informatie gedurende een bepaalde tijd bij het bestuursorgaan beschikbaar blijft en niet bijvoorbeeld automatisch worden overschreven in het kader van periodieke schoning van het systeem. In de rechtspraak is erkend dat het bestuursorganen maatregelen moeten treffen om ervoor te zorgen dat digitale bestanden waaromtrent een Wob-verzoek is gedaan voorhanden blijven, bijvoorbeeld door het maken van een print. Met andere woorden, vanaf het moment dat een Wob-verzoek is ingediend, bijvoorbeeld om een uitdraai te krijgen van de websites die in een analyse zijn meegenomen, zullen conserverende maatregelen moeten worden getroffen om de informatie voorhanden te houden. De jurisprudentie laat zien dat het hierbij niet alleen gaat om een verbod om de opgevraagde documenten vanaf het Wob-verzoekmoment te vernietigen, maar ook om een actieve zorgplicht om de opgevraagde documenten actief te conserveren. Dat noodzaakt ten aanzien van iColumbo kortom tot een actief informatiebeheer ten behoeve van de verantwoording en rechterlijke toetsing die voortvloeit uit de Wob. Zodra sprake is van een Wob-verzoek zullen de automatisch gelogde gebruiksgegevens beschikbaar moeten blijven en mogen deze niet langer in het kader van periodieke schoning van het systeem overschreven worden. Bestanden die op het moment van het verzoek reeds gewist zijn, hoeven naar verwachting niet teruggehaald te worden, aangezien dit veelal bijzondere expertise verlangt en daarmee als onevenredige inspanning kan worden aangemerkt.[88]

[85] Reinsma & Van der Sluijs 2002, p. 18.
[86] Zie voor een nadere bespreking van de rechtspraak op dit punt: Daalder 2011, p. 140-141.
[87] Zie voor de verschillende verwijzingen: G. Overkleeft-Verburg in haar noot onder ABRvS 12 oktober 2005, JB 2005/326.
[88] Zie ook Overkleeft-Verburg in haar noot bij ABRvS 16 augustus 2006.

5.4. Bestuurlijke aangelegenheid

Een volgend criterium dat de werkingssfeer van de Wob regelt betreft het begrip 'bestuurlijke aangelegenheid' (art. 3, eerste lid, Wob). Het verzoek om informatie neergelegd in documenten dient namelijk een bestuurlijke aangelegenheid te betreffen. Hiervan is sprake bij 'een aangelegenheid die betrekking heeft op beleid van een bestuursorgaan, daaronder begrepen de uitvoering en voorbereiding daarvan.' De Wob kan buiten toepassing blijven wanneer de informatie geen betrekking heeft op een bestuurlijke aangelegenheid. Kijkend naar de werking van iColumbo/iRN, zal veel informatie echter betrekking hebben op beleid van betrokken (eind)gebruikers, zeker ook omdat hieronder wordt begrepen de voorbereiding en uitvoering van dat beleid – bijvoorbeeld opsporing en handhaving. Daarmee valt het binnen de Wob.

Deze conclusie kan bovendien worden getrokken nu het begrip 'bestuurlijke aangelegenheid' in de jurisprudentie extensief wordt uitgelegd. 'Een vaak gekozen invalshoek is dat de rechter onderzoekt of de gevraagde informatie betrekking heeft op de wijze waarop het bestuursorgaan omgaat met een bepaalde aangelegenheid. (…) Ook wordt wel eens overwogen dat het gaat om gegevens die "zien" op een bepaalde publieke taak, zoals informatie over gebruikte meetapparatuur bij verkeersovertredingen, die ziet op de publieke taak van het OM om door middel van handhaving van de verkeersveiligheid te bevorderen.'[89] Relevant is daarbij ook dat het niet uitsluitend behoeft te gaan om vastgesteld beleid. Ook informatie die aanleiding zou kunnen zijn tot beleid valt binnen de reikwijdte van het begrip. Zo oordeelde de Afdeling Bestuursrechtspraak van de Raad van State dat informatie over de wijze waarop een politiekorps omgaat met vuurwapendiefstallen, waaronder het opnemen van aangiften daarvan en het gevolg dat daaraan al dan niet wordt gegeven, op grond van de Wob vrijgegeven diende te worden omdat deze informatie als een bestuurlijke aangelegenheid moet worden aangemerkt.[90] Andere voor het onderhavige onderzoek illustratieve gevallen waarin het bestaan van een bestuurlijke aangelegenheid werd aangenomen zijn het opsporings- en vervolgingsbeleid van de politie[91] en processen-verbaal en mutatiegegevens die de door de politie gehanteerde strategie bij de handhaving van de openbare orde inzichtelijk maken[92]. Uitsluitend in de gevallen waarin echt iedere relatie met beleid ontbreekt, lijkt de rechtspraak te willen erkennen dat er geen sprake is van een bestuurlijke aangelegenheid.[93]

Ten slotte is het relevant hier te vermelden dat informatie afkomstig van derden buiten de overheid (die als zodanig geen betrekking heeft op een bestuurlijke aangelegenheid) toch onder het bereik van een 'bestuurlijke aangelegenheid' kan komen te vallen wanneer ze verweven raakt met bestuurlijke documenten, en wel vanaf het moment dat deze informatie wordt betrokken bij activiteiten van een bestuursorgaan. Met andere woorden, ook informatie afkomstig van private partijen en verzameld via iColumbo-tools die wordt ingezet door de politie of een andere publieke eindgebruiker kan binnen het bereik van een 'bestuurlijke aangelegenheid' komen te vallen. Illustratief is het oordeel van de Rechtbank Rotterdam in 2004, waarin werd vastgesteld dat een overheidsdatabank die door de overheid in samenwerking met private partijen en met gegevens van deze partijen was gevuld, aan te merken viel als een bestuurlijke aangelegenheid.[94]

Al met al is duidelijk dat er rekening mee gehouden dient te worden dat informatie over de keuzes en strategieën die voortvloeien uit de inzet van iColumbo onder het bereik van de Wob kan vallen en daarmee openbaar zou kunnen worden. Dat geldt ook voor informatie die met behulp van andere HDIeF-tools wordt gegenereerd. Dit bereik maakt de vraag des te belangrijker in welke situatie een beroep kan worden gedaan op de uitzonderingegronden van de Wob, bijvoorbeeld omdat openbaarmaking in strijd zou zijn met de privacy van betrokken personen dan wel het opsporingsbelang zich tegen openbaarmaking verzet.

5.5. Openbare informatie

Kenmerkend voor iColumbo/iRN is dat deze systemen gebruik maken van informatie die grotendeels al openbaar is. Immers, de informatie wordt hoofdzakelijk verzameld uit openbare

[89] Daalder 2011, p. 162.
[90] ABRvS 16 december 2009, LJN BK6722.
[91] Rb. Den Haag 16 september 2009, LJN BG2031.
[92] ABRvS 20 januari 2010, LJN BK9880.
[93] Een voorbeeld hiervan is ABRvS 17 september 2008, AB 2008, 331 m.nt. P.J. Stolk.
[94] Rb. Rotterdam 19 januari 2004, LJN AO2362.

Internetbronnen. Het is vaste jurisprudentie dat de Wob niet van toepassing is op openbare informatie, bijvoorbeeld omdat deze informatie vrij toegankelijk is dan wel voor iedereen opvraagbaar is (zoals informatie bij de KvK). Dit uitgangspunt blijkt echter niet zo geïnterpreteerd te kunnen worden dat informatie die door een bestuursorgaan in het publieke domein is verzameld, daarmee automatisch als openbare informatie gekwalificeerd kan worden.[95] Met andere woorden, indien een derde inzicht wenst te verwerven in de openbare bronnen die door een overheidsdienst zijn gebruikt en verzoekt om de Internetbronnen beschikbaar te stellen die in het kader van iColumbo/iRN zijn benut, kan het argument niet zijn dat van openbaarmaking geen sprake behoeft te zijn omdat deze bronnen al openbaar zijn. Het gaat immers niet zo zeer om de informatie uit de bron zelf, als wel om de informatie dat die Internetpagina als bron is gebruikt door toepassing van iColumbo/iRN, inclusief mogelijk beschikbare contextinformatie als zoekvraag en beschikbare loggegevens.

5.6. Uitzonderingsgronden

Belangrijk is de vraag welke belangen dan wel welke andere wetgeving derogeert aan het systeem van de Wob. In het geval van iColumbo/iRN gaat het dan om sectorregelingen als de Wet politiegegevens en de Wiv 2002. Ook gaat het om belangen als de persoonlijke levenssfeer en het opsporingsbelang. Vermeld moet direct wel worden dat de uitzonderingen op de Wob restrictief worden geïnterpreteerd. Zo werd het openbaarmakingsbelang uit het oogpunt van goede en democratische bestuursvoering mede in verband gebracht met het toenemend beleidsmatige karakter van de inzet van politiecapaciteit.[96]

5.6.1. Sectorwetgeving gaat voor Wob

Allereerst zal voor de drie eindgebruikers die in deze studie primair worden geanalyseerd, worden bezien in hoeverre specifieke wetgeving derogeert aan de Wob.

Politie

Wat betreft gegevens die gebruikt worden door de politie speelt de vraag of de Wob van toepassing is dan wel het verstrekkingenregime van de Wet politiegegevens (WPolG). Het antwoord hangt af van de kwalificatie van deze gegevens als politiegegeven. In par. 4.1 is opgemerkt dat de persoonsgegevens die na zoekacties via iColumbo beschikbaar komen en waar eventueel vervolgens bewerkingen op plaatsvinden onder de Wet politiegegevens vallen. De Afdeling Bestuursrechtspraak heeft overigens duidelijk gemaakt dat bij een verzoek om informatie over bij de politie rustende gegevens telkens nauwkeurig vastgesteld moet worden welke informatie exact onder het regime van de Wet politiegegevens valt en welke niet – en daarmee onder het regime van de Wob.[97] Daarbij heeft de Afdeling de nodige ruimte gelaten aan het belang van openbaarmaking van gegevens, met als gevolg kritische reacties binnen de politiewereld.[98] Wat volgens Overkleeft-Verburg in de kritiek meespeelde 'is de latente vrees dat een ruimere toepassing van de Wob via "fishing expeditions" oneigenlijk (activistisch) gebruik uitlokt, terwijl het politie(informatie)belang bij geheimhouding op basis van de wettelijke weigeringsgronden van de Wob onvoldoende zou zijn verzekerd.'[99] In tegenstelling tot de eerdere Wet politieregisters, bevat de WPolG overigens geen expliciete regeling voor de relatie met de Wob en blijft in afwachting van nadere rechtspraak rechtsonzekerheid bestaan over de relatie tussen beide wetten.[100]

Belastingdienst (regulier alsook FIOD)

Artikel 67 Algemene wet rijksbelastingen (AWR) vormt een bijzondere, van de Wob afwijkende regeling. Deze regeling geldt sinds enkele jaren zowel voor de gevallen waarin het informatie over de verzoeker zelf betreft als situaties waarin derden om informatie vragen.[101]

[95] ABRvS 6 januari 2010, LJN BK8363.
[96] Overkleeft-Verburg, noot onder ABRvS 16 augustus 2006.
[97] ABRvS 19 mei 2010, LJN BM4969.
[98] ABRvS 29 november 2006, LJN AZ3237.
[99] Overkleeft-Verburg 2007.
[100] Ibid.
[101] Wet van 27 september 2007, *Stb.* 2007, 376.

MIVD
Voor documenten die bij de inlichtingen- en veiligheidsdiensten berusten is via de Wiv 2002 een bijzondere regeling voor openbaarmaking getroffen. In plaats van het adagium van de Wob 'openbaar, tenzij…' geldt hier 'geheim, tenzij…'.[102] De Wiv 2002 maakt daarbij een onderscheid tussen persoonsgegevens en andere gegevens. Het opvragen van persoonsgegevens is slechts mogelijk voor de betrokkene zelf (art. 47 Wiv 2002). Voor de overige gegevens geldt dat deze opgevraagd kunnen worden door eenieder, waarbij de uitzonderingsgronden (art. 55 en 56 Wiv 2002) identiek zijn aan de uitzonderingsgronden van de Wob (waarvan hieronder de belangrijkste voor iColumbo worden besproken). Relevant voor iColumbo is de uitzonderingsgrond van het belang van de nationale veiligheid, waar onder meer het belang van bronbescherming en het belang van gehanteerde werkwijzen onder vallen.[103]

Uit het voorgaande wordt duidelijk dat waar het gegevens betreft die na zoekacties via iColumbo beschikbaar komen, deze veelal niet onder het regime van de Wob zullen vallen. Dat betekent echter geenszins dat allerhande andere informatie zoals in de inleiding van deze paragraaf opgesomd, wel onder het regime van de Wob kan vallen. Voor deze informatie is de vraag van belang of andere belangen dan dat van openbaarheid verstrekking op grond van de Wob zouden kunnen tegenhouden. Te denken valt bijvoorbeeld aan een overzicht van de personen die concreet het systeem hebben gebruikt. Het systeem logt zoals besproken alles en daarmee is deze informatie in principe achterhaalbaar. Nu het hier persoonsgegevens van individuen betreft is een belangrijke vraag welk belang prevaleert: openbaarheid of persoonlijke levenssfeer?

5.6.2. Andere belangen dan openbaarheid prevaleren
Hierna zullen de voor iColumbo relevante relatieve uitzonderingsgronden worden behandeld. Er zal daarbij altijd sprake moeten zijn van een afweging tussen de verschillende belangen die aan de orde zijn. Hiernaast gelden voor enkele situaties absolute uitzonderingsgronden (art. 10, eerste lid, Wob), waarbij voor iColumbo met name relevant is de absolute uitzonderingsgrond voor bijzondere persoonsgegevens (als bedoeld in art. 16 Wbp). Concreet betekent het dat wanneer na zoekacties via iColumbo gegevens over iemands strafrechtelijke achtergrond beschikbaar komen, deze niet via een Wob-verzoek openbaar kunnen worden. Daarbij moet overigens worden vermeld dat deze absolute uitzonderingsgrond in de rechtspraak beperkt wordt uitgelegd en wel zodanig dat 'het enkele feit dat er enig verband is tussen de informatie en een tegen verzoeker aangespannen strafzaak niet voldoende' is.[104] Binnen de reikwijdte van bijzondere persoonsgegevens – en daarmee de absolute uitzonderingsgrond van de Wob – vallen ook gegevens over ras of afkomst, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging.

Wat betreft de absolute uitzonderingsgronden moet verder het belang van de veiligheid van de staat nog worden genoemd. Hieronder wordt mede begrepen de bestrijding van terrorisme. De belangen van strafrechtshandhaving vallen hier niet onder. In dit geval moet een beroep worden gedaan op de relatieve uitzonderingsgrond van art. 10, tweede lid, onder c Wob: het belang van de opsporing en vervolging van strafbare feiten.

Belangrijker zijn daarom ook deze en andere relatieve uitzonderingsgronden van art. 10 tweede lid, Wob. Indien een bestuursorgaan een beroep doet op een dergelijke uitzonderingsgrond en een verzoek tot openbaarmaking afwijst, waarna dit besluit wordt bestreden bij de rechter, zal deze laatste het besluit toetsen door bij de belangenafweging het belang van de openbaarheid voorop te stellen ('openbaar, tenzij…') en vervolgens na te gaan of het bestuursorgaan voldoende heeft gemotiveerd dat de uitzondering ('tenzij…') aan de orde is. Dat verlangt kortom dat het bestuursorgaan concretiseert en preciseert waarom de uitzondering aan de orde is. Hieronder worden kort twee uitzonderingen die met name voor iColumbo relevant zijn, besproken.

5.6.3. Opsporingsbelang
Het belang van de opsporing en vervolging van strafrechtelijke feiten wordt als uitzonderingsgrond erkend via art. 10, tweede lid, onder c, Wob. Het betreft hier een relatieve

[102] Zie onder meer ABRvS 16 april 2008, *JB* 2008/126.
[103] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 69.
[104] Daalder supra p. 318 voetnoot 171 over ABRvS 3 september 2003, LJN AI1749.

uitzonderingsgrond, wat betekent dat het belang van strafrechtelijke rechtshandhaving afgewogen moet worden met het belang van het verstrekken van de informatie. De uitzonderingsgrond geldt zowel voor het belang van opsporing en vervolging in concrete gevallen als in het algemeen.[105] In het laatste geval kan het bijvoorbeeld gaan over een onderzoeks- en opsporingsstrategie van de politie[106] of informatie die inzicht biedt in vertrouwelijke opsporingsmethoden.[107] In de literatuur wordt aangenomen dat alhoewel naar de letter van de wet de uitzonderingsgrond niet ziet op het beschermen van het belang van het *voorkomen* van strafbare feiten, het onwenselijk zou zijn als preventie niet via de uitzondering wordt afgedekt.[108] De rechtspraak lijkt daar geen probleem van te maken.[109]

Deze uitzonderingsgrond zal, mits voldoende beargumenteerd, ingeroepen kunnen worden door de politie en bijzondere opsporingsdiensten; iColumbo verschilt in dit opzicht niet van andere systemen of strategieën die opsporingsinstanties hanteren.

5.6.4. Persoonlijke levenssfeer

Het belang van de persoonlijke levenssfeer kan bij iColumbo voor twee typen individuen relevant zijn: a) personen over wie met behulp van iColumbo informatie wordt gegenereerd en b) personen die gebruik maken van iColumbo. Wat betreft het eerste type personen zal de hiervoor besproken sectorspecifieke regelgeving (zoals de WPolG) veelal derogeren aan de Wob. Voor de situaties dat de Wob wel van toepassing is, geldt dat telkens weer de concrete omstandigheden van het geval bij de beoordeling een rol zullen spelen: weegt gegeven de omstandigheden het belang van de bescherming van de persoonlijke levenssfeer op tegen het belang van publieke controle? Nogal privacygevoelige gegevens, waar – gegeven het oogmerk van het systeem – bij iColumbo sprake van zal kunnen, zullen minder openbaar gemaakt moeten worden (zeker als het verzoek afkomstig is van een derde en niet de betrokkene zelf) dan minder privacygevoelige gegevens.

Als de persoonsgegevens betrekking hebben op de individuen die gebruik maken van iColumbo (wie heeft wanneer, welke zoekacties via het systeem uitgezet) is het uitgangspunt in de jurisprudentie dat de persoonlijke levenssfeer niet in het geding is wanneer iemand uitsluitend beroepshalve opereert. Wel laat de rechtspraak van de laatste jaren een duidelijke tendens zien 'naar het meer beschermen van namen van ambtenaren of werknemers van ondernemingen, ook al gaat het uitsluitend om het beroepshalve functioneren van de betrokkenen.'[110] De persoonlijke levenssfeer wordt met name als uitzonderingsgrond aangenomen als het verzoek tot openbaarmaking zich juist richt op de namen van ambtenaren (bijvoorbeeld namen van belastingambtenaren met het oog op een procedure, of namen van sociaal rechercheurs).[111] In lijn met deze jurisprudentie mag worden verwacht dat als het openbaarmakingsverzoek expliciet ziet op de namen van ambtenaren die in een bepaalde zaak iColumbo hebben ingezet, openbaarmaking zal worden geweigerd. Wel is daarentegen niet geheel uit te sluiten dat een lijst met namen van iColumbo-gebruikende individuen moet worden verstrekt als het verzoek ziet op het toetsen van de bevoegdheid om iColumbo in te zetten. Zo mochten de namen van leerkrachten in combinatie met het al dan niet hebben van een lesbevoegdheid openbaar worden.[112] Volgens de Rechtbank was onvoldoende inzichtelijk gemaakt waarom de docenten onevenredig werden benadeeld als de gegevens over hun bevoegdheid openbaar worden gemaakt.

Afrondend kan worden vastgesteld dat de laatste tijd de jurisprudentie een teneur heeft om terughoudender te zijn met openbaarmakingsverplichtingen, met het oog op het belang van de persoonlijke levenssfeer. Het blijft echter altijd een relatieve uitzonderingsgrond waarbij nog steeds het belang van openbaarheid voorop staat. De vraag die daarom telkens beantwoord zal moeten worden is of het privacybelang dusdanig groot is dat dit zwaarder moet wegen dan de bijdrage die openbaarmaking levert aan de controle op de publieke sector. Daarbij zal gekeken

[105] Zie voor een overzicht van de welke gevallen waarin een openbaarmakingsverzoek wel c.q. niet werd gehonoreerd: Daalder 2011, p. 338-339.
[106] ABRvS 30 juli 2008, LJN BD8907.
[107] ABRvS 4 februari 2004, LJN AO2833 en AO2838.
[108] Daalder 2011, p. 336.
[109] Daalder 2011, p. 336.
[110] Daalder 2011 p. 357.
[111] Daalder 2011 p. 357.
[112] Rb. Alkmaar 4 mei 2011, LJN BQ4168.

moeten worden naar de concrete omstandigheden, zoals het type persoonsgegevens. Ook is relevant of anonimiseren een optie zou kunnen zijn.

5.6.5. Informatie ten behoeve van intern beraad

Een laatste uitzondering die hier wordt besproken is die betreffende persoonlijke beleidsopvattingen ten behoeve van intern beraad. Ook binnen iColumbo zal sommige informatie mogelijk kunnen kwalificeren als informatie opgesteld in het kader van intern beraad met persoonlijke beleidsopvattingen over de onderzoeksmethoden en de wijze van verslaglegging van deze methoden. Dergelijke informatie behoeft niet te worden openbaargemaakt. Het zal dan concreet gaan om persoonlijke meningen van bij iColumbo/iRN betrokkenen over de wijzen waarop het onderzoek kan worden uitgevoerd en daarvan verslag kan worden gedaan.

5.7. Conclusie

Bij de ontwikkeling en het gebruik van iRN/iColumbo moet rekening gehouden worden met de Wet openbaarheid van bestuur. Alle beleidsstukken rond de ontwikkeling en het beheer van het systeem zijn in beginsel Wob-baar, behoudens specifieke onderdelen waarvan de bekendmaking de staatsveiligheid of concrete opsporingsbelangen in gevaar zouden brengen. Mutatis mutandis geldt hetzelfde voor onderdelen van het gebruik van iRN/iColumbo, bijvoorbeeld beleidsstukken van eindgebruikers betreffende hun inzet van het systeem. Mogelijk valt ook onder de openbaarmakingsplicht een lijst welke functionarissen het systeem gebruiken, als het Wob-verzoek beoogt de bevoegdheid te toetsen van de eindgebruiker om het systeem in te zetten. Op de binnen iRN/iColumbo verwerkte gegevens (alle gelogde data) zal de Wob vaak niet van toepassing zijn, in elk geval voor eindgebruikers in de opsporings- en veiligheidssector.

Deel II. Waarborgen

In dit deel gaan we in op het tweede deel van de onderzoeksvraag:

> Voor zover er lacunes of onduidelijkheden in de juridische bestendigheid zijn, welke waarborgen kunnen dan worden ingebouwd tegen onwenselijk gebruik of misbruik van de systemen en de daarin verwerkte informatie, gegeven de beoogde primaire eindgebruikers?

De mogelijke waarborgen zijn tweeledig: ex ante / preventief, dat wil zeggen in het systeem in te bouwen waarborgen die misbruik voorkomen (hoofdstuk 6: compliance by design) en ex post / reactief, dat wil zeggen mechanismen om mogelijk misbruik tijdens het gebruik te monitoren en te compenseren (hoofdstuk 7).

6. Privacymaatregelen in het systeemontwerp

Een belangrijke manier om ervoor te zorgen dat wettelijke plichten worden nagekomen, is technologie te gebruiken die naleving afdwingen of faciliteren. Dit wordt vaak aangeduid als 'code as law' of 'techno-regulering'.[113] Privacy is een belangrijk toepassingsgebied van deze benadering, in de vorm van 'privacy by design' en Privacy-Enhancing Technologies. Ook andere wettelijke vereisten (zoals het respecteren van auteursrechten) kunnen in het systeemontwerp worden betrokken. In dit hoofdstuk beperken we ons echter tot het hoofdaspect van dit rapport: privacy.

6.1. Privacyrobuust ontwerpen (Privacy by Design)

Privacy by Design is een ontwerpfilosofie waarbij in een vroeg stadium van het ontwerp van een (IT-)systeem wordt nagedacht over de privacy implicaties en het gebruik van persoonsgegevens binnen dat systeem. Dit maakt het mogelijk om in een vroeg stadium technische en organisatorische voorzieningen te treffen die er toe moeten bijdragen dat het systeem voldoet aan de regelgeving op het gebied van de bescherming van persoonsgegevens in enge zin en in bredere zin de privacy van betrokkenen in het systeem waarborgt.

Privacy by design is in wezen een koepelbegrip waaronder onder meer Privacy Enhancing Technologies (PET) en organisatorische maatregelen vallen. Zowel Privacy by Design als Privacy Enhancing Technologies zijn op de agenda gezet door, onder meer, de Information & Privacy Commissioner van Ontario (Canada), Ann Cavoukian. Zij vat PbD handzaam samen in zeven beginselen:

- Proactief en niet reactief; preventie en niet herstel;
- Privacy als *default*;
- Privacy ingebed in het ontwerp;
- Behoud van volledige functionaliteit; positieve som in plaats van een nulsom;
- *End-to-end* beveiliging – *lifecycle* bescherming;
- Zichtbaarheid en transparantie;
- Respect voor de privacy van de gebruiker.[114]

De proactieve benadering houdt in dat een organisatie vraagt wat de potentiële privacyimplicaties zijn bij de start van het ontwerp van een nieuw systeem, dat wil zeggen zodra begonnen wordt met de organisatie van het bedrijfsproces rond zowel systeemontwikkeling en -gebruik. Het hangt samen met het tweede en derde principe, waarin privacy als vanzelfsprekend uitgangspunt wordt benoemd en waarin privacy van begin af aan bij het systeemontwerp wordt betrokken. Behoud van volledige functionaliteit wijst erop dat op voorhand goed wordt nagedacht over systeemfunctionaliteiten, hetgeen moet leiden tot duidelijke keuzes over welke gegevens voor welk doel worden verzameld. Dit geheel een levert een netto positief resultaat op: de organisatie kan doen wat het wil doen en de privacy van het individu over wie gegevens worden verzameld wordt beschermd. De begin-tot-eind- en levenscyclusbescherming houdt in dat over alle onderdelen en stadia van het proces wordt nagedacht, en dat adequate maatregelen worden getroffen om gegevens te vernietigen (of onomkeerbaar anonimiseren) aan het eind van de cyclus, dat wil zeggen wanneer ze tot hun doel hebben gediend. Zichtbaarheid en transparantie en respect voor de privacy van de gebruiker wijzen op het perspectief van degenen om wie het gaat, die moeten (kunnen) weten wat er met hun gegevens gebeurt. Ontwerpers moeten zich daarom inleven in de positie van betrokkenen (de datasubjecten) als zij nadenken over het systeem dat zij ontwerpen.

Als geheel drukken deze beginselen uit dat privacybescherming een belangrijke rol moet spelen bij het *ontwerp* van een systeem, en niet pas als het ontwerp al af is en het systeem op de markt wordt gezet of in gebruik wordt genomen. Ook moet het systeem privacymaatregelen en regelgeving zo veel mogelijk 'afdwingen' door systeemkeuzes en –beperkingen.

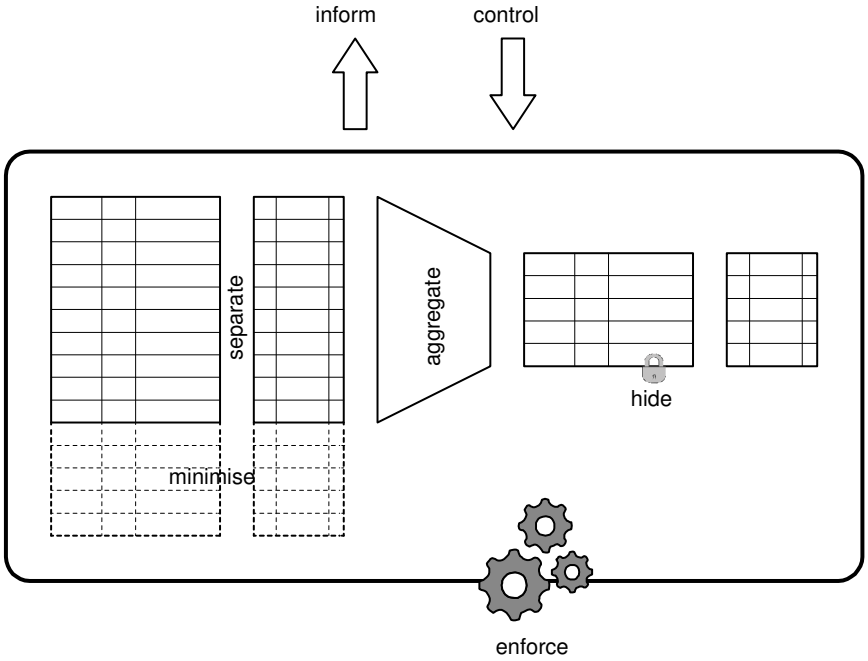
[113] Lessig 1999; Leenes 2010.
[114] Cavoukian 2010. Zie ook Van Lieshout e.a. (2012), die een nadere uitleg van en invulling aan de beginselen geven.

6.2. Privacybeschermende technologieën (PETs)

Privacy Enhancing Technologies (PETs) kunnen gebruikt worden om de privacy van een systeem te verhogen. Deze PETs kunnen het best geïmplementeerd worden tijdens de ontwikkeling van een systeem. Dit geeft invulling aan het idee van PbD, waardoor de privacy beter beschermd blijft in het systeem.

6.2.1. Privacy-ontwerpprincipes[115]

PETs kunnen worden ingedeeld in zeven principes. Deze principes zijn weergegeven in Figuur 2. Ieder principe is een uitgangspunt voor de ontwikkeling van het systeem, waarbij de privacyvriendelijkheid verhoogd wordt. Door het gebruik van een goede combinatie van deze principes, kan de functionaliteit van het systeem bewaard blijven terwijl de bescherming van privacy verbetert. In de volgende subparagrafen zullen we deze principes toelichten, en bij ieder principe aangeven aan welke conceptuele mogelijkheden te denken valt om het principe mogelijk te implementeren binnen iColumbo.



Figuur 2: Privacy design principes

Minimalisatie

Minimalisatie houdt in dat er zo min mogelijk informatie verzameld en verwerkt wordt. Een beperking in de hoeveelheid informatie die verzameld wordt, betekent een beperking van de privacyimpact. Een belangrijke afweging hierbij is echter wel dat het verzamelen van (grote hoeveelheden) informatie de kern vormt van iColumbo, en het moeilijk is om de dataverzameling te minimaliseren zonder dat dit (te veel) ten koste gaat van de functionaliteit. Het is echter wel mogelijk om selectief te zijn in de informatie die verzameld wordt. Zo kan ervoor gekozen worden dat er alleen gericht naar persoonsinformatie gezocht wordt als er een voldoende aanleiding voor bestaat (bijvoorbeeld een redelijke verdenking). Het systeem zou ook de gebruiker kunnen alerteren wanneer hij herhaaldelijk naar dezelfde persoon zoekt (waardoor de zoekvraag sneller het karakter van stelselmatige observatie zal krijgen) en vragen of hij hiervoor voldoende autorisatie heeft (bijvoorbeeld een bevel van de officier van justitie of toestemming van het afdelingshoofd of de privacyfunctionaris). Dit zou zelfs kunnen worden afgedwongen in het systeem door herhaald zoeken op dezelfde persoon (binnen een bepaalde periode) te vereisen dat vooraf aangewezen personen hiervoor specifiek toestemming hebben gegeven, hetgeen te

[115] Deze paragraaf bouwt voort op het werk van Jaap-Henk Hoepman, gepubliceerd in B.J. Koops et al. (2012).

automatiseren valt via beleidsprotocollen en het gebruik van een Privacy Policy Enforcement Language.[116]

Verder moet er bij minimalisatie ook aandacht gegeven worden aan het verwijderen van informatie wanneer deze niet meer nodig is voor het onderzoek. Uitgangspunt hierbij moet zijn om informatie zo kort mogelijk op te slaan.

Een andere mogelijkheid is om (een deel van) de persoonsgegevens geanonimiseerd of gepseudonimiseerd op te slaan. Technisch gezien is het mogelijk automatisch namen te herkennen waardoor het mogelijk is om een groot gedeelte van de namen in de data die worden verwerkt zodanig te veranderen dat ze niet meer herleidbaar zijn tot concrete individuen. Met de huidige stand van de techniek is het niet mogelijk om identificerende gegevens al in het stadium van geautomatiseerde verzameling en verwerking te pseudonimiseren, aangezien dan data uit verschillende bronnen over dezelfde subjecten niet met elkaar in verband kunnen worden gebracht als de identificerende gegevens verschillen (bijvoorbeeld spellingsvarianten of spelfouten). Pseudonimisering is wel een oplossing bij de opslag van gegevens nadat analisten data gecontroleerd en waar nodig met elkaar in verband hebben gebracht. Afhankelijk van de context en het doel van het onderzoek kan ervoor worden gekozen om de pseudonimisering onomkeerbaar of omkeerbaar te doen. In het eerste geval kunnen de data niet terugherleid worden (althans in theorie; juist bij grote databestanden bestaat een risico dat door combinatie van gegevens heridentificatie toch weer mogelijk wordt[117]). Gegevens kunnen dan langer worden bewaard, aangezien anonieme data niet herleidbaar zijn tot personen en dus niet vallen binnen de reikwijdte van de Wbp. Problematisch is wel dat naamherkenning niet perfect is en in de praktijk slechts 80%-90% van de namen herkend en veranderd zal worden. Voor de Wbp levert dit, bij de huidige stand van de techniek, vermoedelijk dan niet een voldoende anonimisering op om het databestand als geheel langer te kunnen bewaren dan noodzakelijk voor het oorspronkelijke doel.

Bij omkeerbare pseudonimisering kunnen gegevens wel terugherleid worden tot identificeerbare personen. Er is dan eigenlijk geen sprake van dataminimalisatie, maar van het principe van verbergen (zie onder), waarbij alleen geautoriseerde personen toegang kunnen hebben tot de gedepseudonimiseerde data.

Scheiding

Het scheidingsprincipe houdt in dat persoonsgevoelige informatie afgescheiden verwerkt wordt. Op deze wijze wordt voorkomen dat er een volledig profiel van een gebruiker wordt gemaakt, waarbij bijvoorbeeld links worden gelegd tussen een belastingonderzoek en een justitieel onderzoek. Dit principe wordt in beginsel al toegepast binnen iColumbo in de vorm van een scheiding tussen eindgebruikers, die verzamelde data niet van elkaar te zien kunnen krijgen (eindgebruikers willen of mogen meestal niet met elkaar delen welke onderzoeken zij precies uitvoeren). Ook het gebruik van zaakdossiers met toegangscontrole (zie Bijlage 1) is een vorm van toepassing van het scheidingsprincipe. Niettemin is er nog de nodige speelruimte voor uitwisseling van gegevens; eindgebruikers willen bijvoorbeeld wel informatie delen over welke identiteiten bij elkaar horen. In welke mate de uitwisseling van gegevens wordt toegestaan is een beleidskeuze die binnen iColumbo moet worden gemaakt. Gemaakte keuzes kunnen vervolgens technisch worden afgedwongen met behulp van toegangscontrole en een Privacy Policy Enforcement Language.

Aggregatie

Aggregatie houdt in dat persoonsgevoelige informatie samengevoegd wordt op een hoger abstractieniveau. Het resultaat kent daarbij een lager detailniveau maar is nog steeds functioneel voor het beoogde doel. Een voorbeeld is het gebruik van gegevens uit energiemeters van huishoudens om piekbelasting op te vangen; hiervoor is het niet nodig om gegevens per afzonderlijk huis te verwerken maar volstaat het om op bijvoorbeeld straat- of wijkniveau gegevens te aggregeren. Deze gegevens zijn dan geen persoonsgegevens meer omdat zij niet zijn te herleiden naar individuele personen.

[116] Bijvoorbeeld XACML (eXtensible Access Control Markup Language), zie Ardagna et al. 2007, of EPAL (Enterprise Privacy Authorization Language), zie http://www.zurich.ibm.com/security/enterprise-privacy/epal/.
[117] Ohm 2010.

Voor iColumbo kan aggregatie voor sommige eindgebruikers toegepast worden wanneer zij niet geïnteresseerd zijn in specifieke individuen, maar meer in objecten of tendensen. Het detecteren van een tendens houdt in dat persoonsgevoelige informatie van individuen samengevoegd wordt, en hierin één gezamenlijke tendens herkend wordt. Voor een trendanalyse is aggregatie een effectieve privacybeschermende technologie.

Verbergen

Het verbergen van informatie houdt in dat informatie alleen zichtbaar is wanneer dat echt noodzakelijk is. Informatie die niet noodzakelijk zichtbaar is voor iedere gebruiker, is alleen zichtbaar voor de gebruiker voor wie dit wel noodzakelijk is. Voor iColumbo betekent dit dat een gebruiker alleen in dossiers kan kijken waar hij zelf bij betrokken is. Zelfs binnen dossiers kunnen namen afgeschermd worden (pseudonimisering) wanneer er geen reden is om deze zichtbaar te maken voor een specifieke gebruiker.

Informeren[118]

Het is voor burgers van belang om op de hoogte te zijn van de informatie die over hen verwerkt wordt. Op deze wijze blijft het systeem transparant, en weet de burger waar hij aan toe is. Informatieplichten en inzagerechten zijn ook opgenomen in privacywetgeving. In het geval van iColumbo zal het informeren van individuen van wie gegevens worden verwerkt niet aan de orde zijn, deels vanwege bescherming van belangen van het lopende onderzoek, deels vanwege de praktische onmogelijkheid om alle individuen te notificeren. Wel is het mogelijk om de burger in het algemeen op de hoogte te brengen van het iColumbosysteem en van welke overheidsdiensten voor welke doeleinden van dit systeem gebruik maken. Inzagerechten zijn mogelijk wel iets om bij het systeemontwerp rekening mee te houden. Burgers kunnen op basis van de Wbp (en in sommige gevallen op basis van de WPolG of Wiv 2002) verzoeken aan een iColumbo-gebruiker of deze gegevens over hem verwerkt en zo ja welke. Het systeem moet dan zodanig zijn ingericht dat deze informatie zonder veel moeite gegenereerd kan worden.

Controle

Het controleprincipe geeft aan dat een burger invloed heeft op de informatie die over hem verwerkt wordt. Dit kan betekenen dat hij de informatie mag corrigeren, maar ook mag verzoeken om de informatie te laten verwijderen uit het systeem. Dit controleprincipe hangt samen met het principe over informeren, omdat deze controle alleen uitgeoefend kan worden als een burger weet welke gegevens over hem worden verwerkt. Omdat bij de uitoefening van correctierechten vaak een waardering moet plaatsvinden of het verzoek terecht is en of een uitzonderingsgrond van toepassing is, valt het moeilijk te automatiseren. Ook is het moeilijk toepasbaar bij de logfunctie voor bewijsdoeleinden en Replay-functionaliteit, aangezien daar de data zoals oorspronkelijk verzameld ongewijzigd voor moeten blijven. Niettemin is het van wezenlijk belang voor burgers om hun correctierecht en verzoekmogelijkheid tot verwijdering te kunnen uitoefenen, bijvoorbeeld in gevallen van persoonsverwisseling, maar ook gezien de vervuiling of veroudering van informatie uit open bronnen. Het systeem moet daarom wel een mogelijkheid kennen om onjuiste of verouderde gegevens (als deze niet gecorrigeerd of verwijderen kunnen worden) als zodanig te markeren.

Hier liggen overigens ook kansen voor iColumbo om correctierechten van burgers juist beter te kunnen honoreren. Slachtoffers van identiteitsdiefstal hebben vaak moeite om structureel uit bestanden van bijvoorbeeld politie of kredietbureaus te komen.[119] iColumbo zou een mogelijkheid kunnen inbouwen om openbroninformatie die suggereert dat een bepaalde persoon mogelijk slachtoffer is van identiteitsdiefstal, te gebruiken om deze persoon te markeren in het systeem, zodat gebruikers met bijvoorbeeld een waarschuwingsicoontje worden gealerteerd op de mogelijkheid dat er sprake is van persoonsverwisseling.

Afdwingen

Afdwingen is een belangrijk principe om ervoor te zorgen dat gemaakte afspraken en regels ter bescherming van de privacy daadwerkelijk worden nageleefd. Het afdwingen kan binnen

[118] Zie ook hfd. 7 over transparantie.
[119] Van der Meulen en Koops 2011.

iColumbo een belangrijke positie innemen, als versterking van de andere principes. Dit afdwingen houdt bijvoorbeeld in dat een gebruiker die een deel van de informatie niet in mag zien, technisch ook niet in staat is om deze informatie in te zien, en dat hij alleen die functionaliteiten kan gebruiken waarvoor hij geautoriseerd is. Dit kan afgedwongen worden door middel van een inlognaam en wachtwoord, maar ook fijnmaziger door het gebruik van een privacybeleidsprotocol dat wordt geïmplementeerd met behulp van een Privacy Policy Enforcement Language.

6.3. Conclusie

In dit hoofdstuk is het concept privacy by design toegelicht en zijn een aantal principes genoemd voor Privacy Enhancing Technologies die de privacy-compliance van iColumbo kunnen verhogen. Niet al deze principes zijn even goed toepasbaar op iColumbo, zoals de principes van informeren of controle, omdat deze in strijd kunnen komen met functionele eisen van het systeem. Maar andere principes zijn zeer goed van toepassing op iColumbo, zoals het scheidingsprincipe, het verbergen en het afdwingen. Deze principes dwingen af dat een gebruiker alleen de informatie kan verzamelen die noodzakelijk is voor het uitvoeren van zijn opsporings/handhavingstaak. Ook kan iColumbo door middel van logging de controleerbaarheid verhogen of de eindgebruiker zich wel aan de regels gehouden heeft.

Het toepassen van de genoemde principes is altijd een contextspecifieke exercitie waarbij veelal ook afwegingen moeten worden gemaakt. Niet altijd kunnen alle principes volledig ingevuld worden. Ook zal per eindgebruiker verschillen welke principes in welke mate en op welke manieren toegepast kunnen worden. Duidelijk is wel dat veel van de principes in elk geval tot op zekere hoogte toegepast kunnen worden, niet alleen door eindgebruikers zelf maar ook in het systeemontwerp van iColumbo. Het verdient daarom aanbeveling om bij elk principe een nadere analyse uit te voeren of en hoe dit in het systeem kan worden toegepast.

7. Transparantie en accountability

7.1. Inleiding

ICT kan een waardevolle bijdrage leveren aan opsporing en rechtshandhaving, maar de toepassing ervan creëert een complexe werkelijkheid. De WRR concludeerde in haar rapport *iOverheid* uit 2011 dat er een toenemende uitwaaiering van individuele ICT-toepassingen en een verknoping van informatiestromen plaatsvindt tussen verschillende publieke en private actoren. Dit maakt de verantwoordelijkheidsverdeling complex en onduidelijk. De WRR benadrukt in zijn rapport het belang van een bewuste en expliciete afweging tussen verschillende beginselen en wettelijke vereisten, die toetsbaar zijn en publiekelijk verantwoord moeten worden. De invulling van die toetsing en verantwoording kan daarbij verschillen per type overheidstaak. De algemene principes van *good governance* (legitimiteit, accountability, transparantie, integriteit en onpartijdigheid) liggen ten grondslag aan het raamwerk dat de WRR heeft geformuleerd.

In deze paragraaf gaan wij in het bijzonder in op transparantie en accountability. Transparantie en verantwoording afleggen over de verwerking van persoonsgegevens zijn niet alleen belangrijk vanuit de wettelijke vereisten in de Wet bescherming persoonsgegevens, maar ook voor de legitimiteit van overheidshandelen, het vertrouwen van burgers in de overheid en de acceptatie van het overheidssysteem door burgers. In deze paragraaf kijken we vanuit dit oogpunt naar de ontwikkeling en het gebruik van het iRN/iColumbo-systeem. Eerst lichten we de belangrijkste begrippen toe. Vervolgens gaan we in op het belang van transparantie en het belang van accountability bij de verwerking van persoonsgegevens.

7.2. Begripsbepaling[120]

7.3.1. Legitimiteit

Het begrip legitimiteit wordt op verschillende manieren omschreven, vaak afhankelijk van het toepassingsgebied of de wetenschappelijke discipline waarin het wordt gebruikt. De term stamt van het Middeleeuws Latijnse *legitimatus,* voltooid deelwoord van *legitimare*: legitimeren. De Merriam-Webster Online Dictionary geeft als secundaire betekenissen voor het Engelse 'legitimate' onder andere:

- precies zo zijn als bedoeld: niet vervalst of onecht;
- in overeenstemming met het recht of bestaande wettelijke vormen en vereisten of heersend krachtens of op grond van een strikt erfelijk recht;
- in overeenstemming met erkende beginselen of gedeelde regels en maatstaven.

Het gebruik van het begrip in de politicologie sluit hierop aan: het duidt op het recht of de bevoegdheid van een staat of regering om macht uit te oefenen. Daarbij wordt legitimiteit gebruikt in een meer globale of dispositionele betekenis en in een meer lokale of handelingsgebonden betekenis. Vedder zegt hier over: 'In de eerstgenoemde betekenis wordt de betrokken overheid en haar handelen als geheel gekwalificeerd. In de laatstgenoemde betekenis gaat het om specifieke (typen of clusters van) handelingen. Zo kan een overheid over het geheel genomen wel legitiem zijn, maar incidenteel een *faux pas* maken uit een oogpunt van legitimiteit'.[121]

Bij legitimiteit kan onderscheid gemaakt worden tussen empirische en normatieve benaderingen van legitimiteit.[122] Normatieve benaderingen richten zich op *idealen*; empirische benaderingen draaien rond de *feitelijke* motieven en oorzaken van de perceptie van burgers van overheden als zijnde legitiem. De normatieve benadering richt zich op acceptatie door burgers van overheidshandelen voor zover dit voldoet aan morele en juridische maatstaven. Het gaat om de vraag: met welk recht oefent de overheid macht uit? Deze maatstaven zijn in vorige hoofdstukken in detail aan de orde gekomen. Daarin werd duidelijk dat gebruik van iRN/iColumbo gelegitimeerd is als voldaan wordt aan wettelijke eisen als vastgelegd in bijvoorbeeld de Wbp, Auteurswet en Wet politiegegevens, maar dat de rechtmatigheid niet altijd duidelijk is,

[120] Deze paragraaf is gebaseerd op Vedder 2011.
[121] Vedder 2011.
[122] Steffek 2003.

bijvoorbeeld bij intensief gebruik van iRN/iColumbo voor de algemene politietaak, bij gebreke aan een expliciete wettelijke grondslag.

Bij de empirische benadering ligt de focus op de psychologische, sociologische en politieke factoren en mechanismen die de perceptie van legitimiteit bij burgers teweeg brengen. Het gaat om legitimiteit als praktisch fenomeen en om overwegingen van politieke doelmatigheid en effectiviteit. Deze aspecten zullen centraal staan in deze paragraaf. Uit verschillende incidenten blijkt dat overheidsbeslissingen over ICT-systemen (al dan niet gelegitimeerd door democratische besluitvorming) soms moeten worden herzien vanwege maatschappelijke weerstand. Burgers hebben bijvoorbeeld geen vertrouwen in het systeem of zien andere bezwaren tegen het overheidsbesluit. Vertrouwen, tevredenheid en acceptatie worden daarom ook gezien als drie verschillende dimensies van legitimiteit.[123]

7.3.2. Accountability

Accountability kan in het Nederlands vertaald worden als verantwoordelijkheid of het zich kunnen verantwoorden. Verantwoordelijkheid staat voor de plicht of de bereidheid om verantwoording af te leggen: openheid, uitleg, verklaring of motivatie geven voor het eigen handelen of beleid. Het kan deel uit maken van de morele dimensie van legitimiteit.[124] Accountability is ook gerelateerd aan transparantie; door de eigen processen, besluitvorming en afwegingen openbaar en inzichtelijk te maken, wordt het voor burgers of de media mogelijk deze te controleren en de overheid publiek verantwoording af te laten leggen over de uitgevoerde handelingen. Accountability lijkt ook een belangrijk onderdeel te gaan vormen van de herziening van de Europese dataprotectierichtlijn.[125] Het principe betekent dat de verantwoordelijke voor de gegevensverwerking effectieve en passende maatregelen treft om de plichten uit de dataprotectiewetgeving uit te voeren en dat hij in staat is om dit aan te tonen als dit wordt gevraagd (bijvoorbeeld door de toezichthouder).

7.3.3. Vertrouwen

Voor vertrouwen bestaan vele verschillende definities en opvattingen. Het kan betrekking hebben op sociaal of intermenselijk vertrouwen, institutioneel vertrouwen (vertrouwen van burgers in de sociale, economische en politieke instituties van een maatschappij) of vertrouwen in een artefact of object (bijvoorbeeld technologie). Vertrouwen van burgers in de overheid en een overheidssysteem wordt bepaald door een breed scala aan factoren, variërend van eigenschappen van de vertrouwende persoon (ervaring, natuurlijke geneigdheid tot vertrouwen) en factoren van de te vertrouwen persoon/entiteit (zoals reputatie, status) tot externe factoren buiten de vertrouwende en te vertrouwen persoon of entiteit. Hierbij valt bijvoorbeeld te denken aan de goede resultaten die van de interactie tussen de te vertrouwen persoon of entiteit en de vertrouwende persoon verwacht worden.[126] Maar ook de aan- of afwezigheid van formele of informele *reguleringsarrangementen* zoals recht en branchecodes speelt een grote rol.

Vertrouwen in de overheid kan worden aangetast door incidenten als datalekken of ophef over complexe ICT-trajecten als het Elektronisch Patiëntendossier of de OV-chipkaart. Uit verschillende perceptieonderzoeken blijkt dat de specifieke context, de aard van (of het type) persoonsgegevens en het doel van de verwerking van persoonsgegevens de attitude over het gebruik van persoonsgegevens beïnvloeden.[127] Koffijberg en anderen vonden dat als belangrijke factor voor de acceptatie van de verwerking van persoonsgegevens vooral controle en transparantie naar voren komt.[128] In het algemeen is het vertrouwen van burgers, ook in Nederland, in de overheid en verschillende overheidsinstanties hoger dan dat in commerciële partijen als het gaat om het gebruik en verwerking van persoonsgegevens.[129] Wat betreft vertrouwen in instituties blijkt dat Nederlanders, op de radio na, het meest vertrouwen hebben in

[123] Tyler 1990.
[124] Vedder 2008.
[125] Zie Proposal for a General Data Protection Regulation, 25.1.2012, COM(2012) 11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
[126] Laufer en Wolfe 1977.
[127] TNS-NIPO 2011; Attema en de Nood 2010.
[128] Koffijberg et al. 2009.
[129] Gallup 2008.

de politie (73%), gevolgd door het leger (71%); vertrouwen in het rechtssysteem staat op de vijfde plaats (65%).[130]

7.3. Het belang van transparantie

In de vorige hoofdstukken is beschreven aan welke juridische criteria systemen als iRN/iColumbo moeten voldoen. Zoals uit de bovenstaande omschrijving van legitimiteit duidelijk wordt, is dit juridische kader evenwel maar een deel van het verhaal. Legitimiteit wordt ook beïnvloed door andere aspecten, zoals de mate van transparantie over het systeem, de mate van vertrouwen van burgers in de rechtsstaat en justitie, de mate waarin de overheid verantwoording aflegt over de ontwikkeling en het gebruik van het systeem en de mate waarin burgers het gebruik van een dergelijk systeem acceptabel vinden. Transparantie is daarmee een onderdeel van het noodzakelijke stelsel van *checks and balances*, dat het mogelijk maakt de motivatie, de achtergrond en het proces van besluitvorming te controleren. Op die manier kan transparantie helpen bij het voorkomen van machtsmisbruik door de overheid. Transparantie bij opsporing en rechtshandhaving vraagt om een andere invulling dan transparantie bij overheidsdienstverlening: een verdachte zal veelal niet gaande het onderzoek worden geïnformeerd over het onderzoek en alle gegevens die over hem of haar bekend zijn. Er kan wel op andere manieren openheid worden geboden, bijvoorbeeld door op algemeen niveau inzicht te geven in de manier waarop een systeem als iRN/iColumbo wordt gebruikt tijdens de opsporing. Het is daarom van belang dat bij het gebruik van iRN/iColumbo openheid wordt betracht over de voorwaarden en vormen van gebruik en het proces dat gevolgd wordt. Bij deze transparantie kan ook worden gewezen op andere toezichtsmechanismen die worden aangebracht om het systeem evenwichtig en controleerbaar te maken (zie par. 7.4).

In de laatste decennia is men in verschillende landen begonnen systemen te ontwikkelen die zich richten op het beter en efficiënter kunnen doorzoeken van de groeiende hoeveelheid (digitale) gegevens, met het oog op de handhaving van de rechtsorde en het beschermen van de nationale veiligheid. Deze systemen hebben een vergelijkbare doelstelling als iRN/iColumbo. Een aantal daarvan zijn echter gestopt vanwege grote maatschappelijke weerstand. Gebrek aan transparantie over de ontwikkeling, besluitvorming en aangebrachte of benodigde waarborgen, evenals morele bezwaren van burgers over het gebruik van dergelijke systemen, waren daarvoor belangrijke oorzaken. Negatieve media-aandacht over het systeem speelde een belangrijke rol om maatschappelijke organisaties en de betrokken parlementen te activeren.

De evaluaties van verschillende stopgezette systemen (zie Kader 1 en 2) maken duidelijk dat de projecten enerzijds te weinig aandacht hebben besteed aan bestaande privacywetgeving en daaruit voortvloeiende privacyrisico's, en anderzijds leden aan een gebrek aan transparantie, democratisch toezicht en publieke communicatie over de ontwikkeling en het gebruik van het systeem. In verschillende gevallen is met de ontwikkeling van het systeem begonnen zonder medeweten of toestemming van het parlement.

Total Information Awareness

In de Verenigde Staten is in 2002 na de aanslagen van 9/11 het programma Total Information Awareness (TIA) opgericht als een vijfjarig onderzoeksprogramma. TIA bracht verschillende technologieën vanuit het onderzoeksinstituut van het Ministerie van Defensie bij elkaar in een experimenteel prototype om terroristische aanslagen tijdig op te kunnen sporen en te voorkomen. TIA zou gebruik maken van verschillende typen databronnen, waaronder openbroninformatie, data afkomstig van inlichtingendiensten en biometrische gegevens. In november 2002 schreef journalist William Safire een invloedrijk stuk over TIA in de *New York Post* dat duidelijk maakte dat de Amerikaanse overheid deze technologie ook kon inzetten op haar eigen burgers. Dit creëerde veel negatieve media-aandacht. Het Ministerie van Defensie veranderde de naam van het programma naar 'Terrorist Information Awareness' om beter aan te geven wat het doel was van het programma. Als gevolg van de media-aandacht werd het programma kritisch gevolgd door consumentenorganisaties en actiegroepen als ook het Amerikaanse Congres. Het Congres vroeg om inzicht in de effectiviteit, financiering en privacyimplicaties van het programma. Na het ontvangen van deze informatie besloot het Congres het programma te beëindigen, nog geen jaar

[130] SCP 2011.

na de start van het programma, vanwege zorgen over schending van privacy en andere burgerrechten. In een evaluatie van het programma concludeerde het Ministerie van Defensie dat, hoewel het programma positief had kunnen bijdragen aan de strijd tegen het terrorisme, het onderzoeksinstituut de maatschappelijke gevoeligheden beter had kunnen adresseren om zo mogelijk machtsmisbruik door de overheid te voorkomen. Er werden overheidsfinanciën ingezet voor een systeem dat nooit volledig bruikbaar zou zijn zonder kostbare en ingewikkelde herzieningen en 'reparaties' achteraf. Een tweede evaluatie van de, door het Congres ingestelde, adviesraad over TIA concludeerde dat TIA een 'gebrekkige poging was een strevenswaardig doel te bereiken'.[131] Het was gebrekkig vanwege de ongevoeligheid van het ministerie ten aanzien van kritieke privacykwesties, de manier waarop het programma werd gepresenteerd aan het publiek en het gebrek aan duidelijkheid en consistentie in de beschrijvingen van het systeem. De Commissie benadrukte het belang van een transparant politiek proces en duidelijke bestuurlijke en juridische supervisie om een herhaling in de toekomst te voorkomen.

Kader 1: Total Information Awareness (Verenigde Staten) – stopgezet in 2003

EDVIGE

In Frankrijk werd in 2008 EDVIGE opgericht. Dit bestond uit software ontwikkeld voor de Franse nationale politie voor het analyseren van gegevens over personen die mogelijk gevaarlijk zijn (met betrekking tot de nationale veiligheid) en voor (in het verleden) gekozen of toekomstige politici of personen met een institutionele, religieuze of economisch belangrijke rol.[132] Het systeem was bedoeld om profielen of dossiers op te bouwen om politie en inlichtingendiensten te voorzien van relevante informatie. Er kwamen veel negatieve reacties vanuit de samenleving, zowel vanuit nationale en internationale instituties als maatschappelijke organisaties. Een van de klachten was bijvoorbeeld een gebrek aan publieke consultatie over de ontwikkeling en toepassing van het systeem. Ook het parlement was niet betrokken geweest bij de ontwikkeling van het systeem. De Verenigde Naties veroordeelden het project als een schending van het Internationaal verdrag inzake burger- en politieke rechten uit 1966.[133] Om die redenen werd het systeem aangepast, maar dit betroffen nauwelijks substantiële herzieningen. In november 2008 is het programma teruggetrokken. Een latere versie, EDVIRSP, onderging het zelfde lot.

Kader 2: EDVIGE (Frankrijk) – stopgezet in 2008

Uit evaluaties van de stopgezette systemen komt ook de roep om toepassing van Privacy Enhancing Technologies (PET's) en Privacy by Design (PbD) naar voren. PET's en PbD kunnen helpen om overheidsmisbruik te voorkomen door het aanbrengen van benodigde (privacy)waarborgen (zie hfd. 6). Deze technieken kunnen daarmee de legitimiteit van een overheidssysteem bevorderen. In 1999 werd door de Kamer de motie-Nicolai aangenomen, waarin de overheid verplicht werd om in nieuwe systemen Privacy Enhancing Technologies toe te passen. In de praktijk gebeurt dit echter nog nauwelijks. Een recent kleinschalig onderzoek over het vertrouwen van burgers in Privacy by Design laat overigens zien dat de aanname dat PET's en PbD acceptatie van systemen zouden verhogen niet per se klopt.[134] In het onderzoek is gekeken naar verschillende elementen van PbD, waaronder Privacy Impact Assessments (PIA's), organisatorische maatregelen (zoals het aanstellen van functionarissen voor de gegevensbescherming, het melden van datalekken en dergelijk) en het toepassen van PET's. De verschillende elementen lijken elk een ander effect te hebben op vertrouwen en acceptatie van burgers in het overheidssysteem. (Hierbij moet wel worden aangetekend dat de resultaten uit dit onderzoek zijn verkregen uit focusgroepen en nog onder een representatieve groep van de bevolking nader kwantitatief gevalideerd dienen te worden.)

Vooral die elementen van Privacy by Design die transparantie van gegevensverwerking door de overheid vergroten, lijken een positief effect te hebben op vertrouwen van burgers in de overheid. Dit zijn onder andere het uitvoeren en publiceren van een PIA en organisatorische

[131] TAPAC 2004.
[132] Zie G. Davet, 'Edvige: le projet de décret de Michèle Allot-Marie', *Le Monde*, 18 september 2008, http://www.lemonde.fr/societe/article/2008/09/18/edvige-le-projet-de-decret-de-michele-alliot-marie_1096633_3224.html.
[133] Zie http://www.nonaedvige.sgdg.org/spip.php?article209.
[134] Kool et al. 2011.

maatregelen zoals het geven van toegankelijke informatie over de gegevensverwerking, het duidelijk vragen van toestemming daarvoor, en het instellen van een eenvoudig te vinden contactpunt voor vragen of klachten. Het laten uitvoeren van de PIA door een onafhankelijke organisatie levert ook een positieve bijdrage aan het vertrouwen. Het uitvoeren van een PIA bij publieke diensten lijkt voor burgers extra van belang, omdat daar vaak geen alternatieve dienstverlener is en burgers verplicht zijn de dienst af te nemen (zoals de OV-chipkaart of vingerafdrukken in het paspoort). Ook worden de verzamelde gegevens bij overheidsdiensten doorgaans als gevoeliger van aard beschouwd. Wettelijke verplichtingen die de verantwoordelijkheden van organisaties vastleggen en vergroten, alsmede het actief uitdragen van de naleving daarvan, kunnen ook positief bijdragen aan vertrouwen van burgers in publieke diensten. Sterk onafhankelijk toezicht is daarvan een voorbeeld. Uit de voorbeelden van buitenlandse systemen blijkt dat dit toezicht vaak ontbrak: het systeem werd ontwikkeld zonder toestemming of medeweten van het parlement.

In hoofdstuk 6 zijn verschillende – technisch in te bouwen – waarborgen genoemd die privacyrisico's kunnen verkleinen en voorkomen, bijvoorbeeld door (gedeeltelijke) anonimisering van gegevens en het automatisch afdwingen van toegangsbevoegdheden tot bepaalde gegevens afhankelijk van een toegewezen rol. Het eerder genoemde onderzoek van TNO en TILT laat echter zien dat het inbouwen van technische waarborgen vaak 'onder de motorkap' wordt geregeld en dat dit veelal niet zichtbaar of herkenbaar is voor de burger.[135] Privacybeschermende technologie is daarnaast moeilijk te begrijpen voor een leek en wordt als een soort zwarte doos ervaren. De burger kan dus zelf niet goed inschatten wat het gebruik van deze technieken nu echt bijdraagt. In het onderzoek wordt het voorbeeld van *bodyscanners* gebruikt, waarbij een van de aspecten in de privacyvriendelijke variant is dat niet het lichaam wordt getoond, maar slechts een silhouet. De deelnemers aan de studie twijfelden aan de effectiviteit van de privacyvriendelijke scanner en gaven de voorkeur aan de niet-privacyvriendelijke oplossing. Het inbouwen van privacytechnieken leidt daarmee dus niet per definitie tot een hogere acceptatie van burgers; minstens zo belangrijk als PET's en PbD is daarom een open en adequate communicatie over gemaakte keuzes en ingebouwde waarborgen.

Dit heeft ook gevolgen voor hoe het beste kan worden gecommuniceerd over de toepassing van deze technologie. De wijze van communicatie en de mate waarin de toegepaste waarborgen zichtbaar gemaakt kunnen worden aan het publiek, beïnvloeden de mate van acceptatie van de dienst. Communicatie over de juridische verplichtingen van de eindgebruikers, de aangebrachte waarborgen om overheidsmisbruik te voorkomen (zowel technisch en organisatorisch) en openheid over de ontwikkeling en de condities waaronder het systeem gebruik wordt, zijn daarbij van groot belang.

7.4 Accountability

Legitimiteit van initiatieven verlangt dat daarover rekenschap afgelegd kan worden (*accountability*). De notie accountability sluit nauw aan op de toetsbaarheid die door transparantie mogelijk wordt gemaakt, maar voegt daar bindende consequenties ('afrekening') aan toe. Achter het brede begrip *accountability* verschuilen zich allerhande verschillende belangen, zoals controleerbaarheid, aansprakelijkheid en afrekenbaarheid. Accountability is sterk verbonden met het begrip verantwoordelijkheid. Overduidelijk roept de inzet van technologie en daarmee systemen als iRN/iColumbo vragen en dilemma's op over verantwoordelijkheid, verantwoording nemen en verantwoording afleggen. Hoe meer partijen bij het gebruik en de inzet van de tools samenwerken, des te complexer de vragen over verantwoordelijkheid worden. Wie naar informatieketens kijkt, ziet dat de verantwoordelijkheid voor de technische uitvoering op de ene plaats wordt belegd, terwijl als het aankomt op zaken als informatiebeheer, informatiegebruik en daarbij behorende bevoegdheden, vele andere instanties wat betreft verantwoordelijkheid in beeld zijn. [136] Daar waar op de werkvloer beslissingen genomen worden op basis van informatie aangeleverd door informatiestelsels, en in het geval van iRN/iColumbo ook allerhande bronnen op Internet, is de verleiding groot de verantwoordelijkheid af te schuiven op deze systemen, in de veronderstelling dat de benodigde waarborgen voor naleving van wetgeving wel door het systeem en/of de beheerorganisatie zullen zijn geregeld. Hierdoor zinkt afrekenbaarheid en beheersbaarheid weg in de veronderstelde autonomie van de tools en de hapklare presentatie

[135] Kool et al. 2011.
[136] Zie hierover WRR 2011.

van resultaten uit de afgezochte Internetbronnen. Het feit dat de beslissingen over burgers weliswaar worden genomen aan de hand van informatie gegenereerd met iRN/iColumbo, maar uiteindelijk feitelijk worden genomen door (niet-digitale) samenwerkende overheidsactoren raakt zo buiten zicht. Problematisch in relatie tot *accountability* is ook dat het achterhalen en aanspreken van de verantwoordelijken voor bepaalde 'input' zoals Internetbronnen ingewikkeld is en ook steeds complexer wordt, mede omdat de inputdimensie van zowel openbare bronnen als interne informatiesystemen lang niet altijd eenvoudig te doorgronden zal zijn.

De WRR presenteerde in 2011 in het rapport *iOverheid* zowel transparantie als *accountability* als belangrijke instrumenten wanneer afweging gemaakt worden tussen enerzijds het belang van veiligheid en handhaving (criminaliteitsbestrijding) en anderzijds het belang van privacy. Dit door de WRR gepresenteerde kader beoogt de kwaliteit van de discussie en besluitvorming over de ontwikkeling en inzet van digitale handhavingsinstrumenten zoals iRN/iColumbo te faciliteren. Zowel transparantie als *accountability* zijn – in de terminologie van de WRR – als procesmatige beginselen van doorslaggevend belang voor de instandhouding van een goede balans tussen de stuwende beginselen (zoals criminaliteitsbestrijding en rechtshandhaving) en verankerende beginselen (zoals privacy, maar ook autonomie van de professionals binnen eindgebruikers). Ook kan het een leidraad bieden voor het daaraan voorafgaande proces van zoeken en bediscussiëren van een balans. Ook dienen ze ter waarborging van de toetsbaarheid van het proces van ontwikkeling van tools als iRN/iColumbo. Transparantie eist zo dat de partners die deze tools inzetten de afwegingen die ze vaak impliciet genoodzaakt zijn te maken bij de inzet van deze tools, te expliciteren en controleerbaar te maken. Accountability verlangt dat ze over alle keuzes en afwegingen verantwoording kunnen afleggen.

Accountability kan in relatie tot de inzet van iRN en iColumbo langs twee wegen een rol spelen. In een politieke vorm – bijvoorbeeld via parlementaire controle en ministeriële verantwoordelijkheid – is het een belangrijk instrument voor het toetsen van de bevoegdheden van de partners die bij de inzet van het systeem zijn betrokken en de afwegingen die ze daarbij maken. In zijn juridische vorm is *accountability* instrumenteel voor de mogelijkheden van burgers om uitkomsten van iRN/iColumbo-gebruik aan te vechten. Als *accountability* bij de inzet van de tools voldoende is gewaarborgd, heeft de burger overigens niet alleen kans om voor zijn individuele belangen op te komen. Er ontstaat ook, 'door de optelsom van acties van burgers, een kritisch tegenwicht dat behulpzaam kan zijn voor het versterken van de inhoudelijke kwaliteit van de relatie burger-overheid in het digitale tijdperk.'[137] Om burgers in staat te stellen tegenwicht te bieden, is openheid van zaken ten aanzien van de inzet van iRN/iColumbo nodig. Zonder transparantie die resulteert in effectief inzicht bij burgers (al dan niet via de band van de controlerende taak van de media), is reëel toezicht onmogelijk. Vanuit zowel transparantie als accountability is het eerder in dit rapport besproken instrument van de Wet openbaarheid van bestuur voor burgers daarom een belangrijk instrument.

Meer concreet kijkend naar iRN/iColumbo spelen transparantie en accountability een rol in de diverse stadia, van de voorbereiding en ontwikkeling van het systeem tot aan de bredere toepassing van deze tools door allerhande partijen. Concreet zouden via beide beginselen,

a. zowel het proces van ontwikkeling van de tools,
b. de keuze voor de inzet ervan door diverse partijen, als
c. de wijze waarop deze partijen de tools uiteindelijk inzetten

inzichtelijk, navolgbaar, bediscussieerbaar en uiteindelijk ook in rechte aanvechtbaar moeten kunnen worden gemaakt. Dat de eisen van transparantie en accountability niet alleen zouden moeten gelden voor de concrete toepassing van de tools door derde partijen, maar ook voor de ontwikkeling daarvan door de initiatiefnemers, voert terug op de overweging dat de ontwikkeling van iRN/iColumbo in feite al een voorschot op de toekomst neemt via het realiseren en faciliteren van de beschikbaarheid van deze tools. Technologie is niet goed of slecht, maar ook niet neutraal.[138] Dat betekent bijvoorbeeld dat bij het proces van ontwikkeling van de tools afwegingen geëxpliciteerd zullen moeten worden rondom kwesties als afgeschermde toegang, het verzamelen van beeldmateriaal, het kunnen negeren van robots.txt-bestanden, de manier en duur van opslag, het delen van informatie over gevonden verbanden tussen entiteiten, enzovoorts. Ook besluiten over een (nieuwe) toepassing van iRN/iColumbo, het formuleren van

[137] WRR 2011, p. 84.
[138] Kranzberg 1986.

de opdracht aan ontwikkelaars, de beslissing om bepaalde bronnen via de tools te laten analyseren dan wel nieuwe organisaties van de tools gebruik te laten maken zullen – met in het achterhoofd de beginselen van transparantie en accountability - inzichtelijk en bediscussieerbaar moeten kunnen zijn.

Als het gaat om de burger als individu, zeker als die zijn recht zoekt omdat hij in zijn belangen wordt geraakt door een beslissing genomen mede op basis van iRN/iColumbo-informatie, is transparantie hoogstens een begin. Met alleen transparantie wordt de burger immers wel gefaciliteerd, maar hij heeft noch de autoriteit noch de doorzettingsmacht om daadwerkelijk iets te wijzigen in de consequenties die de inzet van iRN/iColumbo voor hem kunnen hebben. De praktijk van de inzet van de tools moet dus verder uitgewerkt worden met goede procedures voor eindverantwoordelijkheid, een kenbare ingang om fouten te kunnen laten corrigeren en mogelijkheden om te worden gecompenseerd voor ondervonden nadeel. Daarbij moet een evenwicht gevonden worden tussen de verantwoordelijkheid van de burger om onjuistheden aan te (kunnen) kaarten (bijvoorbeeld omdat blijkt dat de Internetbronnen onjuiste informatie bevatten) en de verantwoordelijkheid van de partijen die de tools gebruiken om fouten ook daadwerkelijk recht te zetten**.** Zeker bij het gevoelige en kwetsbare domein van opsporing en rechtshandhaving (gekenmerkt door een grote winst voor de samenleving bij succes en tegelijk grote repercussies voor het individu bij fouten) kan het niet zo zijn dat de burger moet opdraaien voor (de gevolgen van) foutieve of verouderde informatie die op Internet te vinden is en vervolgens via de tools door gebruikers van de tools wordt ingezet. Kortom, enerzijds is de verantwoordelijkheid van overheid groot omdat alleen zij de doorzettingsmacht heeft om fouten te corrigeren. Anderzijds moet de drempel voor de individuele burger ook niet te laag zijn aangezien dan relatief (te) gemakkelijk grote inspanningen aan de kant van de betrokken partijen worden gevraagd. Dit vraagt om een nadere uitwerking van waarborgen, zowel bij de systeemontwikkeling en het systeembeheer als bij eindgebruik, die leiden tot een evenwichtig en hanteerbaar stelsel van *checks and balances*.

7.5. Conclusie

Zowel de ontwikkelaars en beheerders als de gebruikers van iRN/iColumbo zullen een scherp oog moeten hebben voor de mogelijke negatieve en soms zelfs schadelijke effecten van de inzet van de infrastructuur en de daarop toegepaste tools. Goede procedures om daarmee om te gaan zijn van groot belang voor zowel individuele burgers die mogelijk nadeel kunnen ondervinden van onjuiste beslissingen op basis van iRN/iColumbo-informatie, als ook voor het in stand houden en versterken van vertrouwen in de inzet van de tools in het algemeen. Die procedures vragen om een effectieve uitwerking van de beginselen van accountability en transparantie, waarbij een goede balans moet worden gevonden tussen de rol en verantwoordelijkheid van de diverse betrokken partijen enerzijds en van de burger anderzijds. Het is daarbij van belang om een onderscheid te maken tussen de burgerrol van *citoyen* (politiek subject) en de burger als individu (rechtssubject). In het eerste geval gaat het om de burger als een productieve *countervailing power* die inzicht zou moeten hebben in de ontwikkeling en inzet van de tools, om aldus in het stelsel van *checks and balances* van de democratische rechtsstaat bij te kunnen dragen aan het voorkomen van machtsmisbruik door de overheid. In het tweede geval gaat het om de burger die toegang moet hebben tot het recht wanneer hij vanwege de inzet van de tools onjuist of onheus wordt bejegend door de overheid en onterecht nadeel ondervindt van overheidsbeslissingen.

Deel III. Conclusies en aanbevelingen

8. Conclusies en aanbevelingen

In dit rapport is onderzocht of de binnen het programma HDIeF ontwikkelde producten (iColumbo en in het verlengde daarvan het iRN als centrale infrastructuur en de daarop aan te sluiten modules, hierna gezamenlijk ook aangeduid als 'het systeem') privacybestendig en in overeenstemming met IE- en overige relevante wetgeving zijn. Ook is onderzocht welke waarborgen kunnen worden ingebouwd tegen onwenselijk gebruik of misbruik van het systeem en de daarin verwerkte informatie, gegeven de beoogde primaire eindgebruikers. Aangezien verschillende doelgroepen van dit rapport uiteenlopende informatiebehoeften hebben, wordt het niet zinvol geacht om hier een samenvatting te geven van alle bevindingen uit het rapport; de lezers worden daarvoor verwezen naar de afzonderlijke hoofdstukken die via de inhoudsopgave goed toegankelijk zijn. In plaats daarvan bevat dit hoofdstuk een conclusie in de vorm van een dwarsdoorsnede van juridische aandachtspunten waarmee bij de verschillende onderdelen van iRN/iColumbo rekening mee moet worden gehouden. We onderscheiden daarbij verschillende typen functionaliteiten, op systeemniveau (par. 8.1.1) en op eindgebruikerniveau (par. 8.1.2), alsmede overige aandachtspunten voor systeemontwikkeling en -beheer (par. 8.1.3) en voor eindgebruikers (par. 8.1.4). Mede op basis hiervan formuleren we aanbevelingen voor de betrokken actoren en voor nader onderzoek (par. 8.2).

8.1. Conclusies ten aanzien van systeemontwikkeling en -beheer

8.1.1. Functionaliteiten van zoeken, bewerken en opslaan

Bij het verzamelen van informatie uit open Internetbronnen moeten diverse keuzes worden gemaakt. Ten eerste de vraag **welke (typen) bronnen** kunnen of mogen worden onderzocht. In de interviews voor dit onderzoek bleek verschil van interpretatie te bestaan wat precies een 'open' bron is. Voor de een is dat een Internetpagina die zonder enige drempel toegankelijk is, voor de ander een Internetpagina die voor iedereen toegankelijk is al dan niet na registratie. Bij het systeemontwerp van iRN/iColumbo moet worden afgewogen of ook dit laatste type bronnen gefaciliteerd zal worden door het systeem. Een ander aandachtspunt is of de bron beschikt over 'terms of use', die iets zeggen over het gebruik van de werken en databanken die op de website staan. Wordt de inhoud bijvoorbeeld onder een creative commons-licentie beschikbaar gesteld? Het systeem zou het geautomatiseerd lezen van *terms of use* kunnen faciliteren en daar gebruiksrechten aan koppelen. Een volgende ontwerpbeslissing is hoe omgegaan wordt met indicaties op een webpagina over het al dan niet geïndiceerd mogen worden door webcrawlers (in robot.txt-bestanden of andere metadata). Veel eindgebruikers willen ook informatie halen van pagina's die in robot.txt aangeven dat zij niet door zoekmachines willen worden geïndiceerd; het zou daarbij volgens hen gaan om een verzoek zonder juridische status, zodat iRN/iColumbo vanuit dat perspectief geen rekening zou hoeven te houden met toegangsrestricties in metadata. Binnen de context van dit onderzoek kon de vraag naar de juridische status van robot.txt-restricties niet worden onderzocht, nader onderzoek hiernaar zou welkom zijn.[139]

Een tweede vraag betreft **welk (type) materiaal** kan of mag worden verzameld. Dat is vooral een vraag voor eindgebruikers, omdat het niet op systeemniveau te bepalen valt. Veel materiaal in open bronnen omvat *persoonsgegevens*; de verzameling en verdere verwerking daarvan is toegestaan mits wordt voldaan aan de wet- en regelgeving (hfd. 2). Daarnaast zullen open bronnen ook het nodige materiaal bevatten waarop *auteursrechten* of databankrechten rusten (hfd. 3). Of dat materiaal verzameld mag worden, hangt in eerste instantie af van de beoordeling of een (impliciete) licentie mag worden aangenomen om het materiaal binnen te halen; bij webpagina's waarop kennelijk de rechthebbende zelf het materiaal heeft geplaatst zonder gebruiksvoorwaarden, kan men een impliciete licentie aannemen, maar als de webpagina expliciet auteursrechten voorbehoudt dan wel niet duidelijk is wie het beschermde materiaal heeft

[139] Denkbaar is dat een webbeheerder bijvoorbeeld een onrechtmatigedaadsactie zou kunnen ondernemen tegen het systeem of de eindgebruiker, met het argument dat het niet in het maatschappelijk verkeer betaamt om robot.txt te negeren; er zou dan wellicht ook sprake kunnen zijn van computervredebreuk, als de toegang door een zoekrobot als onrechtmatig wordt bestempeld.

geplaatst, is een impliciete licentie niet direct aannemelijk. In die gevallen is de vervolgvraag of een beperking op het auteursrecht van toepassing is; voor veel eindgebruikers zal art. 22 lid 2 Aw de mogelijkheid scheppen om materiaal te verwerken. De reikwijdte van deze bepaling (wat is een bestuurlijke procedure? wat is openbare veiligheid?) is echter niet helemaal duidelijk; dat zal in de rechtspraktijk verder moeten uitkristalliseren.

Eén categorie gegevens vergt wel een systeemkeuze. *Beeldmateriaal* (foto's en video's) waarop personen te herkennen zijn, bevat niet alleen persoonsgegevens maar in beginsel ook bijzondere (gevoelige) persoonsgegevens, aangezien ras en soms gezondheid uit beelden is af te leiden. Aangezien de verwerking van bijzondere persoonsgegevens aan zeer strikte voorwaarden is gebonden, valt het te overwegen het verzamelen van beeldmateriaal in het systeemontwerp uit te sluiten, dan wel aan strikte gebruikersvoorwaarden te binden. Bij het ontwikkelen en testen van het systeem en tools bestaat geen grondslag voor het verzamelen van beeldmateriaal; dit zal daarom met fictieve gegevens moeten geschieden (dan wel ontheffing bij het CBP moeten worden gevraagd). Sommige eindgebruikers zullen wel onder omstandigheden termen kunnen hebben voor het verwerken van gevoelige gegevens maar ook voor hen zijn de eisen restrictief (een *zwaarwegend* algemeen belang waarvoor verwerking van gevoelige gegevens *noodzakelijk* is). Zolang er geen expliciete wettelijke bepaling is die zegt dat de eindgebruiker voor gemiddelde toepassingen van iRN/iColumbo gevoelige gegevens (beelden) mag verwerken, zal de eindgebruiker daarbij ontheffing moeten vragen aan het CBP, en eveneens waarborgmaatregelen moeten nemen om de privacyinbreuk zo klein mogelijk te houden. In het systeemontwerp kan daaraan tegemoet worden gekomen door als standaardinstelling te hanteren dat beeldmateriaal niet wordt verzameld, tenzij een bevoegde autoriteit bij de eindgebruiker toestemming heeft gegeven. Ook zou het systeem waarborgen kunnen bieden in de vorm van een functionaliteit om gezichten in foto's of video's automatisch te detecteren en vervolgens automatisch onherkenbaar te maken (wellicht omkeerbaar volgens het principe van omkeerbare pseudonimisering, zie par. 6.2.1 onder Minimaliseren en Verbergen).

Een derde vraag betreft welke **zoekmodaliteiten** worden geboden. Hierbij spelen drie aspecten een rol. Ten eerste, hoe intensief en over welke periode wordt er informatie verzameld? Voor de mate van privacyinbreuk van iRN/iColumbo-gebruik maakt het verschil of een zoekvraag eenmalig of periodiek wordt uitgevoerd, en of deze beperkt is tot een geselecteerd aantal bronnen of alle mogelijke bronnen verkent. Naarmate de zoekvraag over een langere periode (periodiek) wordt uitgevoerd en/of meer bronnen omvat, is de privacyinbreuk groter en moet deze inbreuk meer expliciet bij wet zijn voorzien. Hoewel dit moeilijk te kwantificeren valt en het omslagpunt van wat 'voorzienbaar is bij wet' contextafhankelijk is (het is voor de burger, bij gebrek aan een expliciete wettelijke bepaling, meer voorzienbaar dat de AIVD het Internet stelselmatig onderzoekt dan de Belastingdienst of de gemeente bij vergunningverlening), valt het te overwegen om in iRN/iColumbo een onderscheid aan te brengen tussen 'lichte' zoekvragen (die niet gericht naar personen vragen, of die eenmalig en beperkt in omvang zijn) en 'zwaardere' zoekvragen, waarbij voor de laatste het systeem een aanvullende toestemming zou kunnen eisen door een aangewezen bevoegde autoriteit, of tenminste een waarschuwingsscherm kan laten zien dat gebruikers wijst op de noodzaak van een wettelijke grondslag.

In het verlengde hiervan kan ten tweede tegemoet worden gekomen aan de problematiek van auteursrechten, waarbij het binnenhalen van materiaal als zodanig gemakkelijker te rechtvaardigen is (op basis van een impliciete licentie dan wel de wettelijke exceptie van openbare veiligheid of een bestuurlijke procedure) dan het daarop volgende gebruik ervan, zoals (her)verspreiding en vertaling. Het systeem zou dit kunnen reflecteren door bepaald vervolggebruik (zoals verspreiding van resultaten onder een brede kring) niet te ondersteunen of onmogelijk te maken, dan wel door de gebruiker te waarschuwen over mogelijke juridische implicaties wanneer modules bewerkingen van materiaal maken.

Ten derde, in hoeverre kan of mag het zoekproces en de selectie en presentatie van resultaten worden geautomatiseerd en zelflerend worden gemaakt? Enerzijds is het wenselijk dat het systeem 'intelligent' genoeg is om tegemoet te komen aan behoeften van gebruikers voor verzameling, selectie en begrijpelijke presentatie van zoekresultaten. Anderzijds mag geen te grote rol aan de techniek worden toebedeeld, aangezien interpretatie van (de context van) resultaten voorbehouden zou moeten blijven aan mensen; dat vloeit voort uit de dataprotectiebepaling dat beslissingen waaraan rechtsgevolgen zijn verbonden of die burgers in aanmerkelijke mate raken nooit volledig geautomatiseerd mogen worden genomen. Het is ook

relevant om ‘disresponsabilisering’ te voorkomen: het risico dat analisten bij eindgebruikers te veel gaan vertrouwen op wat ‘het systeem’ zegt ten koste van hun eigen verantwoordelijkheidsbesef en expertise. De mate van automatisering en zelflerendheid van het proces van zoeken, selectie- en presentatie is een beleidskeuze die moet worden gemaakt op systeemniveau, en ook periodiek moet worden herzien naarmate nieuwe tools en toepassingen (zoals het toepassen van een ‘crawl extender’) worden toegevoegd. Het kan daarbij nuttig zijn om dit spanningsveld tussen technische en menselijke intelligentie en verantwoordelijkheid expliciet als aandachtspunt mee te nemen in maatregelen ter bevordering van accountability, bijvoorbeeld bij periodieke audits van het systeem en het gebruik daarvan.

Een vierde aandachtspunt is welke **bewerkingen** op gevonden gegevens mogen worden toegepast. Relevant is bijvoorbeeld dat bij het koppelen van (niet tot individuen herleidbare) gegevens uit verschillende bronnen gegevens kunnen ontstaan die wel tot individuen herleidbaar zijn en dus onder de dataprotectiewetgeving vallen. Aangezien bij het meeste gebruik van iRN/iColumbo er toch al standaard rekening mee moet worden gehouden dat er persoonsgegevens worden verwerkt, vergt dit als zodanig geen extra maatregelen. Belangrijker is de vraag welke bewerkingen mogelijk zijn op auteursrechtelijk beschermd materiaal, zoals berichten van nieuwspagina’s. Het ligt voor de hand om bijvoorbeeld buitenlandse pagina’s te vertalen, maar een vertaling is, als een bewerking, een relevante handeling onder het auteursrecht die voorbehouden is aan de rechthebbende. Terwijl er wel uitgegaan kan worden bij reguliere (nieuws)pagina’s van een impliciete licentie om het materiaal binnen te halen, is dat bij vertalingen minder duidelijk. Eveneens is onduidelijk of vertalingen ook onder de beperking ten behoeve van de openbare orde of bestuurlijke procedures gebracht kunnen worden. Naar dit aspect lijkt nader onderzoek wenselijk.

Tot slot is de **opslag** van gegevens van groot belang, maar ook een complex vraagstuk. Met het oog op (mogelijke toekomstige) bewijsvoering, worden alle data uit zoekvragen opgeslagen, zodat met de replay-functie te achterhalen is hoe er precies naar welke data is gezocht en welke selecties en bewerkingen zijn toegepast. De opslag moet dusdanig geschieden dat bewijsbaar is dat de data niet aangepast (kunnen) zijn vanaf het moment van opslag. Aangezien tools of algoritmes in de loop der tijd aangepast kunnen worden, is het van belang ook alle tussenstadia van bewerkingen op te slaan, dan wel alle verschillende versies van tools en algoritmes (onmanipuleerbaar) op te slaan, inclusief tijdstempels.

Niet alle data zullen echter voor bewijs gebruikt worden, en sommige zoekacties zullen ook niet (mede) het doel hebben om informatie te verzamelen die als bewijs in rechte te gebruiken moet zijn. Persoonsgegevens moeten dan in principe vernietigd worden na gebruik. De opslag van data betreft een verwerking van persoonsgegevens die aan de dataprotectiewetgeving moet voldoen. In het algemeen zullen data vernietigd (of onomkeerbaar geanonimiseerd) moeten worden zodra zij niet meer dienen voor het doel waarvoor ze verzameld zijn. De periode daarvan verschilt echter van zaak tot zaak. Ook valt er moeilijk een algemene regel te formuleren voor de *opslagtermijn* van gegevens in het iRN/iColumbo-systeem. De diverse eindgebruikers die op het systeem zijn aangesloten, zijn onderhevig aan verschillende wettelijke regimes met zeer uiteenlopende bewaartermijnen. Wellicht is het mogelijk om per eindgebruiker, en daarbinnen per type onderzoek, doel of medewerker, een standaardbewaartermijn in te stellen, waarvan in omstandigheden (met toestemming van een bevoegde autoriteit) kan worden afgeweken.

Naast de bewaartermijn, is ook de manier van opslag relevant. De opslag moet vanzelfsprekend goed *beveiligd* zijn, zowel tegen externe aanvallen als tegen intern lekken of onbevoegd gebruik. Aangezien het om een zeer grote hoeveelheid data gaat, die kwetsbaar zijn in het kader van lopende onderzoeken, is bovendien een hoog beveiligingsniveau vereist. Gegevens die niet gedeeld mogen worden tussen organisaties, zullen adequaat technisch afgeschermd moeten worden; gezien de diversiteit aan eindgebruikers, die veelal onder verschillende wettelijke regimes vallen, zal als standaard moeten worden gehanteerd dat alle opgeslagen gegevens alleen binnen de organisatie van de eindgebruiker toegankelijk zijn, en daarbinnen mogelijk alleen voor deelgroepen, bijvoorbeeld afhankelijk van autorisaties of per operationeel onderzoeksteam.

Het systeem moet voorts verschillende *modaliteiten van opslag* kunnen faciliteren; bij politiegegevens is bijvoorbeeld relevant dat deze tijdens de reguliere bewaartermijn gebruikt mogen worden voor politieonderzoek, maar na afloop van deze termijn nog vijf jaar bewaard moeten worden ten behoeve van klachtenafhandeling en verantwoording; het systeem moet in

staat zijn om gegevens onder deze verschillende regimes op te slaan. Ook kennen politiegegevens bepaalde coderingen of markeringen (zie par. 4.1.5 en 4.1.6), die in het systeem aangebracht moeten kunnen worden bij bepaalde gegevens.

8.1.2. Overige aspecten van systeemontwikkeling en -beheer

Naast specifieke vragen rond de functionaliteiten die het systeem kent, vergen enkele andere vragen de aandacht bij het ontwikkelen en beheren van iRN/iColumbo. Om te beginnen moet rekening gehouden worden met de Wet **openbaarheid van bestuur**. Alle beleidsstukken rond de ontwikkeling en het beheer van het systeem zijn in beginsel Wob-baar, behoudens specifieke onderdelen waarvan de bekendmaking de staatsveiligheid of concrete opsporingsbelangen in gevaar zouden brengen. Mutatis mutandis geldt hetzelfde voor onderdelen van het gebruik van iRN/iColumbo, bijvoorbeeld beleidsstukken van eindgebruikers betreffende hun inzet van het systeem. Mogelijk valt ook onder de openbaarmakingsplicht een lijst welke functionarissen het systeem gebruiken, als het Wob-verzoek beoogt de bevoegdheid te toetsen van de eindgebruiker om het systeem in te zetten. Op de binnen iRN/iColumbo verwerkte gegevens (alle gelogde data) zal de Wob vaak niet van toepassing zijn, in elk geval voor eindgebruikers in de opsporings- en veiligheidssector.

Als uitgangspunt is gekozen dat alle tools ontwikkeld worden op basis van ***open source*** **software**, mede met het oog op controleerbaarheid van resultaten die als bewijs worden gebruikt in een rechterlijke procedure. De openbaarmaking van broncode kan echter ook nadelige gevolgen hebben voor operationeel onderzoek, met name in de justitie- en nationaleveiligheidssfeer. Dit spanningsveld zou mogelijk opgelost kunnen worden door bijvoorbeeld de ontwikkelde tools zodanig onder eindgebruikers te verspreiden dat deze zelf geen kopieën kunnen maken van de tool (zie par. 3.2.3). De precieze vormgeving daarvan hangt echter af van de specifieke *open source*-licenties en kan, inclusief alternatieve oplossingsrichtingen, nader onderzocht worden door de toolontwikkelaars in samenspraak met auteursrechtspecialisten. Daarnaast is ook hier van belang de verplichting op basis van de Wet openbaarheid van bestuur om op verzoek documenten betreffende bestuursaangelegenheden openbaar te maken; aangezien ‘document’ en ‘bestuursaangelegenheid’ ruim worden uitgelegd, kan hier ook door en voor de overheid ontwikkelde en gebruikte programmatuur onder vallen, in elk geval beleidsstukken die de ontwikkeling van de programmatuur betreffen en mogelijk ook de broncode zelf. De vraag of bij ontwikkelde tools een uitzonderingsgrond van de Wob van toepassing is, zoals staatsveiligheid of opsporingsbelang, kan niet in zijn algemeenheid worden beantwoord en zal per tool moeten worden bezien.

Bij het **testen van het systeem** of van daarop aan te sluiten tools dienen in beginsel geen echte persoonsgegevens uit bestaande Internetbronnen te worden gebruikt, aangezien hiervoor moeilijk een wettelijke grondslag is te vinden. Alleen indien het testen met echte gegevens noodzakelijk is (en dus niet met alternatieve gegevensverzamelingen kan worden uitgevoerd) voor het ontwikkelen van tools die van zwaarwegend belang zijn voor de taakuitvoering van de overheidsinstantie, bestaat een grondslag in art. 8 onder f Wbp; de inbreuk op de privacy moet dan zoveel mogelijk worden gemiminaliseerd door bijvoorbeeld automatisch herkende identificeerbare gegevens onomkeerbaar te pseudonimiseren. In elk geval mogen voor testdoeleinden geen echte gevoelige gegevens (waaronder visuele, zoals foto’s en video’s) worden verwerkt.

Voorts is van belang het iRN/iColumbo-systeem, als het in een voldoende rijp stadium van ontwikkeling is om in gebruik te worden genomen bij opsporingsinstanties (dat geldt reeds voor iRN en zal binnenkort het geval zijn voor iColumbo), te laten toetsen aan de eisen van het Besluit technische hulpmiddelen, voor zover deze toepasbaar zijn op programmatuur. In een **keuringsrapport** (door functionele interpretatie van het Besluit zelf in de reguliere procedure, of door een alternatief keuringsrapport van een EDP-audit-achtige instantie) zou moeten worden vastgesteld dat iRN/iColumbo voldoet aan de (relevante) eisen van het Besluit (zoals niet-manipuleerbaarheid en controleerbaarheid van vergaring en bewerking van gegevens). Dit is nodig om het systeem te gebruiken in de context van stelselmatige observatie, wat een van de meest voor de hand liggende bevoegdheidsgrondslagen is voor iRN/iColumbo-gebruik dat verder gaat dan ‘lichte’ zoekvragen die op basis van art. 2 Politiewet 1993 kunnen worden uitgevoerd (zie par. 4.1).

Voor het **beheer** van het systeem is het van belang een adequaat stelsel van maatregelen te ontwikkelen in het kader van accountability (zie hfd. 7). Bij de verduurzaming van iRN (zie bijlage 1) wordt een ondernemingsmodel ontwikkeld ten behoeve van de continuïteit, kwaliteitsborging en doorontwikkeling van iRN/iColumbo. Het is van groot belang om bij het ontwikkelen van een beheermodel uitvoerig aandacht te schenken aan organisatorisch/institutionele en juridische *checks and balances*. Deze moeten waarborgen dat het systeem en daarop aangesloten modules binnen de grenzen van de wet blijven – iets wat voortdurende aandacht vergt ook nadat het onderhavige rapport zal zijn opgeleverd en geïmplementeerd. Onder andere moet blijvende aandacht worden georganiseerd voor rechten van burgers, zowel om kennis te nemen van het systeem en het gebruik daarvan als om op te komen in rechte tegen dit gebruik wanneer zij in hun belangen worden geraakt. Een stelsel van waarborgmaatregelen kan bijvoorbeeld bestaan uit een periodieke Privacy Impact Assessment, vormen van onafhankelijk toezicht en periodieke audits, en intern tegenwicht in de vorm van een functionaris voor de gegevensbescherming en klachtenprocedures. Dit is niet alleen van belang voor juridische compliance in strikte zin, maar ook om in meer algemene zin de legitimiteit van het systeem te waarborgen, wat van cruciaal belang is voor de maatschappelijke acceptatie van het systeem.

Een specifiek aandachtspunt bij het beheer zal daarnaast nog zijn **welke eindgebruikers toegelaten** worden tot het systeem. De vraag welke eindgebruikers aangesloten (mogen) worden op het systeem wordt momenteel op ad hoc-basis beantwoord, waarbij het uitgangspunt is dat (vooralsnog) alleen Nederlandse overheidsinstanties iRN/iColumbo mogen gebruiken. Gedacht wordt aan de mogelijkheid van uitbreiding met andere overheidsinstanties binnen Europa. Binnen dit onderzoek is niet onderzocht welke instanties precies, en zo ja onder welke voorwaarden, toegang zouden moeten kunnen krijgen tot het systeem. Het is niet op voorhand evident dat alle overheidsinstanties binnen Nederland (zonder meer) aangesloten moeten (kunnen) worden op het systeem; in verband met de eis van 'voorzienbaarheid bij wet' is immers een wettelijke grondslag vereist voor de privacyinbreuk waarmee (intensievere vormen van) iRN/iColumbogebruik gepaard gaan, en niet elke overheidsinstantie zal een voldoende kenbare wettelijke grondslag hiervoor hebben. De uitbreiding naar instanties buiten de directe publieke sector, zoals publiek-private samenwerkingsverbanden, dan wel naar instanties buiten Nederland, kan ook juridische vragen oproepen van legitimiteit, alsmede politiek-bestuurlijke vragen rond 'mission creep', die de maatschappelijke acceptatie van het systeem kunnen beïnvloeden. Daarom verdient het aanbeveling een kader te ontwikkelen voor de toelating van organisaties tot iRN/iColumbo, iets wat in elk geval binnen het project Verduurzaming iRN zal moeten gebeuren maar wat ook op centraal overheidsniveau aandacht verdient.

8.2. Conclusies ten aanzien van gebruik van het systeem

Waar de voorgaande aandachtspunten zowel voor systeemontwikkelaars en -beheerders als voor eindgebruikers relevant zijn – en in samenwerking moeten worden opgepakt – zijn er ook enkele aandachtspunten die vooral voor eindgebruikers van belang zijn. Ten eerste de functionaliteit van **afscherming van afkomst** (IP-adres) die in het systeem als mogelijkheid is opgenomen. Deze functionaliteit zal vooral belangrijk zijn voor opsporings- en veiligheidsdiensten, maar ook andere eindgebruikers kunnen er gebruik van willen maken. Het is belangrijk deze functionaliteit als mogelijkheid en niet als intrinsieke systeemeis op te nemen: het afschermen van de afkomst valt niet onder het 'doorsnee-gebruik' van zoeken in open Internetbronnen en de burger zal over het algemeen niet (hoeven te) verwachten dat overheidsinstanties, anders dan gemiddelde Internetgebruikers, hun pagina's doorzoeken zonder daarbij sporen achter te laten. Het afschermen van afkomst heeft daarom gevolgen voor de redelijke privacyverwachting en zal daarom mogelijk aan zwaardere Wbp-eisen moeten voldoen (zoals het aanvullend informeren van burgers over informatieverwerking en een voorafgaand onderzoek door het CBP, zie hfd. 2). Mogelijk zit er zelfs, zoals in par. 4.1.1 beschreven, een element van misleiding in om informatie te verzamelen zonder dat dit zichtbaar is voor de burger (vergelijk ook de eis bij cameratoezicht in de openbare ruimte dat de camera zichtbaar moet zijn voor de burger). De consequenties hiervan zullen per eindgebruiker verschillen. Ivd's hoeven zich bij informatievergaring niet als zodanig kenbaar te maken en mogen zonder meer deze functionaliteit gebruiken. Bij de politie ligt dat ingewikkelder, omdat het element van eventuele misleiding vraagt om een expliciete wettelijke grondslag (bijv. een bevel van de officier van justitie ex art. 126j Sv). Het zoeken in open bronnen met afgeschermde identiteit is een voorbeeld van

nieuwe ontwikkelingen in de online opsporing waarop de wet BOB niet goed toegesneden is; nadere rechtsontwikkeling op dit punt is dan ook wenselijk. Dat geldt eveneens voor de vergelijkbare vraag of en onder welke voorwaarden de politie gegevens mag verzamelen in voor het publiek na registratie toegankelijke weblocaties en daartoe een account mag aanmaken, al dan niet onder pseudoniem; de grenzen tussen rondkijken, stelselmatig observeren, stelselmatig informatie inwinnen en infiltratie zijn voor deze situatie niet duidelijk getrokken in wetsgeschiedenis of rechtspraak. Ook dit vergt nader onderzoek dan wel een richtinggevende uitspraak van de (hoogste) rechter of wetgever. Voor andere eindgebruikers dan ivd's en politie speelt deze problematiek mogelijk ook; ook zij zullen moeten (laten) bepalen wat het betekent in hun juridische context om bij het zoeken in open bronnen hun afkomst af te schermen.

Een tweede aandachtspunt betreft de **autorisaties** voor functionarissen die bij eindgebruikers het systeem kunnen gebruiken. In sommige contexten zullen alleen bepaald aangewezen, dan wel formeel hiertoe geautoriseerde, personen het systeem mogen gebruiken, en in veel contexten moet mogelijk een onderscheid gemaakt worden naar de reikwijdte van de bevoegdheden (bepaalde functionaliteiten van) het systeem te gebruiken. Aangezien intensief (periodiek, grootschalig of zeer gericht) gebruik meer inbreuk maakt op de privacy, is hiervoor sneller een expliciete wettelijke grondslag nodig, die in de context van eindgebruikers vaak gekoppeld zal zijn aan bepaalde voorwaarden, zoals toestemming van een bepaalde autoriteit. Een autorisatiesysteem biedt dan de mogelijkheid, als het systeem gradaties van zoekfunctionaliteiten faciliteert (zie boven bij zoekmodaliteiten), om autorisaties te koppelen aan zoekmodaliteiten en de naleving hiervan technisch af te dwingen. Een adequaat autorisatiesysteem is daarnaast ook cruciaal voor organisaties met verschillende onderdelen die onder verschillende wettelijke regimes vallen, zoals de FIOD-ECD die deels opsporingsonderzoek doet (WPolG) en deels controle uitoefent (Wbp). Het gebruik van iRN/iColumbo moet dan juridisch en organisatorisch strak worden ingekaderd zodat altijd helder is voor welke taak (en dus onder welk juridisch regime) organisatieonderdelen het systeem gebruiken.

In het verlengde hiervan vraagt het **loggen van systeemgebruik** aandacht. Het systeem voorziet in het standaard loggen van alle activiteiten, met het oog op controleerbaarheid en toekomstig gebruik als bewijs van gevonden informatie, maar dit extensief loggen is – als de loggegevens gekoppeld of te koppelen zijn aan individuele werknemers – een personeelsvolgsysteem dat aan juridische eisen van de Wbp en de Wet op de ondernemingsraden moet voldoen (zie par. 2.3.4).

Een derde aandachtspunt is het **markeren en waar nodig afschermen** van gegevens uit zoekresultaten. Waar het persoonsgegevens betreft hebben individuen inzagerechten en correctierechten. De reikwijdte van deze rechten van betrokken in iRN/iColumbo verschilt echter per eindgebruiker (afhankelijk of deze onder het regime van de Wbp, WPolG of Wiv 2002 valt), waarop uiteenlopende, en niet altijd even eenduidige, uitzonderingsclausules van toepassing zijn. In welke mate burgers recht hebben om een eindgebruiker te vragen welke gegevens over hem geregistreerd staan en om te verzoeken deze gegevens te corrigeren dan wel te vernietigen, vergt nader onderzoek per eindgebruiker. In elk geval zal er op systeemniveau wel een technische mogelijkheid moeten bestaan om inzage te geven en om gegevens te corrigeren, te verwijderen of af te schermen (dat wil zeggen, markeren om de verwerking ervan in de toekomst te beperken). Er moet ook rekening mee worden gehouden dat de herziene Europese dataprotectiewetgeving voor politie en justitie aanvullende eisen stelt aan markeringen van gegevens: tussen verschillende categorieën gegevens al naar gelang de mate van nauwkeurigheid en betrouwbaarheid, tussen persoonsgegevens 'gebaseerd op feiten' en persoonsgegevens 'gebaseerd op persoonlijke beoordelingen', en een duidelijk onderscheid tussen verschillende categorieën personen.

Een hieraan gerelateerde vraag is of en onder welke voorwaarden gegevens **tussen eindgebruikers** kunnen worden **gedeeld**. Als standaard mogen gegevens (zowel zoekvragen als resultaten) niet toegankelijk zijn voor andere eindgebruikers (zie boven onder 'opslag'), maar diverse geïnterviewden geven aan dat sommige gegevens wel gedeeld zouden moeten (kunnen) worden. Zij noemen met name het voorbeeld van verbanden tussen deelidentiteiten, bijvoorbeeld dat A op Facebook dezelfde is als B op Twitter. Het delen van persoonsgegevens tussen organisaties is een complex vraagstuk, zeker in een context waarin organisaties onder verschillende dataprotectieregimes (Wbp, WPolG en Wiv 2002) vallen, dat binnen het bestek van

dit onderzoek niet onderzocht kon worden. Er bestaan zeker de nodige mogelijkheden binnen de wetgeving om gegevens aan andere instanties door te geven; de reikwijdte van deze mogelijkheden toegepast op iRN/iColumbo kan het beste bij elke eindgebruiker zelf in kaart worden gebracht, voortbouwend op het bestaande organisatiebeleid rond het delen van persoonsgegevens.

8.3. Afsluiting

In dit rapport is onderzocht of de binnen het programma HDIeF ontwikkelde systemen, met name iColumbo en in het verlengde daarvan het iRN als centrale infrastructuur, in overeenstemming zijn met wetgeving rond privacy en dataprotectie, auteursrechten en databankrechten, sectorale wetgeving betreffende eindgebruikers en de Wet openbaarheid van bestuur.[140] Aangezien iColumbo en de daarop aan te sluiten modules nog volop in ontwikkeling zijn, valt niet eenduidig te concluderen in welke mate deze aan bestaande wetgeving voldoen. Dat zal mede afhangen van keuzes die in het ontwerp en vervolgens in het gebruik worden gemaakt. Daarnaast is het moeilijk conclusies te trekken over de juridische *compliance* van het systeem, aangezien dat voor een belangrijk deel afhangt van het gebruik en de context van dat gebruik. Afhankelijk van de eindgebruiker zijn hierop immers verschillende juridische regimes van toepassing.

Tegelijk biedt deze situatie de mogelijkheid om de nu gemaakte of nog te maken ontwerp- en gebruikskeuzes mede te stoelen op de in dit rapport gesignaleerde juridische aandachtspunten en randvoorwaarden. Bij ontwerp, beheer en gebruik spelen persoonsgegevens en auteursrechten een belangrijke rol, primair met betrekking tot de gegevens die uit open Internetbronnen worden verzameld, maar secundair ook met betrekking tot gegevens over het systeem en zijn gebruikers zelf. Door tijdig oog te hebben voor deze juridische aspecten en maatregelen te nemen om aan wettelijke plichten te voldoen, kan worden geprobeerd het systeem en het gebruik daarvan zo privacyrobuust mogelijk te maken, volgens het principe van Privacy by Design. Bovendien wordt op deze wijze al in algemene zin geanticipeerd op het voldoen aan de (contextafhankelijke) toepasselijke wettelijke regimes. Die maatregelen zullen waar mogelijk moeten bestaan uit technische (en technisch-organisatorische) maatregelen (Privacy Enhancing Technologies), maar ook uit een adequaat stelsel van toezicht, auditing en andere accountability-faciliterende maatregelen.

Dit is geen eenvoudige opgave. Bij de te maken keuzes zullen diverse belangenafwegingen moeten worden gemaakt, niet alleen tussen juridische eisen enerzijds en operationele belangen anderzijds. Ook juridische eisen zijn niet overal eenduidig of goed te combineren. Juridische eisen voor verwijdering van persoonsgegevens na gebruik kunnen op gespannen voet staan met eisen die worden gesteld aan bewijs in rechtszaken; openbaarheid van broncode met het oog op controleerbaarheid van bewijs kan op gespannen voet staan met geheimhoudingsvereisten in opsporings- en veiligheidswetgeving. Dit vereist een nadere bestudering van de precieze belangen die spelen en een intelligente en creatieve benadering om oplossingen te vinden die niet uitgaan van een *zero-sum*-situatie maar die recht kunnen doen aan verschillende belangen tegelijk. Ook hierbij kunnen het gedachtegoed en de in ontwikkeling zijnde technische hulpmiddelen van Privacy by Design een productieve rol spelen.

Wat daarbij niet uit het oog mag worden verloren is dat de plicht om iRN/iColumbo in overeenstemming te brengen en houden met wetgeving een gezamenlijke opdracht is voor de systeemontwikkelaars, systeembeheersorganisatie en eindgebruikers. In een complex netwerk als het onderhavig dreigt de verantwoordelijkheid van individuele partijen vaak snel onder te sneeuwen onder het collectief als daarbij de verantwoordelijkheden niet expliciet zijn belegd. De systeemontwikkelaars en -beheerders kunnen niet zelfstandig alle nodige beleids- en ontwerpkeuzes maken, aangezien die voor een belangrijk deel afhankelijk zijn van behoeften en wettelijke regimes van uiteenlopende eindgebruikers. Op hun beurt kunnen eindgebruikers zelf geen volledige verantwoordelijkheid dragen voor de juridische compliance van het systeem en alle daarop aangesloten modules, aangezien zij geen volledig zicht hebben op het geheel en ook niet altijd in een vroeg genoeg stadium de ontwikkeling kunnen bijsturen. Het is daarom essentieel dat alle bij iRN/iColumbo betrokken actoren een gezamenlijk gedragen

[140] De lezer dient daarbij rekening te houden met de beperking van dit onderzoek tot Nederlands (en waar relevant Europees) recht. Niet is onderzocht of en op welke manieren iRN/iColumbo raakt aan buitenlandse wetgeving op het gebied van persoonsgegevens of auteursrechten.

verantwoordelijkheidsbesef omarmen, dat zich vertaalt in een gemeenschappelijke *governance*-structuur die zich uitstrekt over zowel het hele ontwikkel- en beheerproces als het gebruik van de infrastructuur en de daarop aan te sluiten tools.

De gemiddelde burger zal niet op de hoogte zijn van alle moderne technische mogelijkheden van openbrononderzoek en daarom ook niet (hoeven te) verwachten dat de overheid op grote schaal gebruik maakt van (intelligente combinaties van) gegevens uit open bronnen. Daarom is naast aandacht voor accountability, en overigens eveneens als onderdeel daarvan, ook transparantie van groot belang. De ontwikkeling van een infrastructuur met allerlei toegevoegdewaarde-functionaliteiten die door een breed spectrum aan overheidsinstanties zal worden gebruikt, moet kortom voldoende worden gelegitimeerd. Het feit dat technische ontwikkelingen allerlei nieuwe vormen van zoeken en combineren van gegevens in open bronnen mogelijk maken, is als zodanig geen voldoende argument om iColumbo te ontwikkelen. Niet alles wat technisch kan, moet per se mogen kunnen. In plaats van een techniek- of aanbodgedreven argumentatie, zou de overheid, en in het bijzonder het primair verantwoordelijke departement, moeten beargumenteren waarom een dergelijk systeem noodzakelijk is te ontwikkelen en te gebruiken in onze democratische samenleving, en waarom de manier waarop het systeem is ingericht voldoet aan de algemene beginselen van subsidiariteit en proportionaliteit. De overheid moet en kan transparant zijn over de ontwikkeling en het gebruik door diverse instanties van iRN/iColumbo en de daarop aangesloten modules in het algemeen, bijvoorbeeld door ruimhartig informatie over het systeem beschikbaar te stellen. Daarnaast moeten overheidsinstanties ook zo transparant mogelijk zijn – wat afhankelijk is van de operationele context – over het gebruik in concrete gevallen, zodat de burger die geraakt wordt door beslissingen genomen mede op basis van iColumbo-informatie in rechte kan opkomen voor zijn legitieme belangen. Transparantie op beide niveaus zal bijdragen aan het legitimeren van het systeem, en daarmee aan de maatschappelijke acceptatie ervan, zeker als bij die transparantie gewezen kan worden op alle preventieve en toezichtsmaatregelen die in het kader van Privacy by Design en accountability worden genomen om iRN/iColumbo zo goed mogelijk te laten voldoen aan bestaande wetgeving en aan de daaraan ten grondslag liggende belangen.

9. Een privacychecklist voor HDIeF-tools

In het verlengde van de analyse in dit rapport kan een afvinklijst worden geformuleerd aan de hand waarvan de privacybestendigheid van in de toekomst te ontwikkelen modules en aanpassingen van de iRN/iColumbo-infrastructuur kan worden bestudeerd.

Privacy algemeen

1. In het kader van de ontwikkeling en het gebruik van iColumbo en daarop aan te sluiten modules moet gespecificeerd en onderbouwd worden:
   a. waarom het noodzakelijk is iColumbo en daarop aan te sluiten modules te ontwikkelen/te gebruiken in een democratische samenleving;
   b. dat met iColumbo en daarop aan te sluiten modules de beoogde doeleinden bereikt kunnen worden waarbij de beginselen van subsidiariteit en proportionaliteit leidend zijn (er is gekozen voor het minst ingrijpende middel en het middel staat in verhouding tot het doel).
2. Bij de ontwikkeling van iColumbo en daarop aan te sluiten modules moet het publiek zo volledig mogelijk geïnformeerd worden over wat het systeem is, waarom/waarvoor het ingezet wordt en door wie.

Bescherming van persoonsgegevens

3. Onder welk wettelijk regime valt de ontwikkeling c.q. het beoogde eindgebruik van iColumbo? Indien het niet uitsluitend onder de politietaak of onder de ivd's valt, gelden vanuit de Wbp de volgende vereisten.[141]
4. Wie is verantwoordelijke, dat wil zeggen degene die doel en middelen van de verwerking van persoonsgegevens vaststelt? Dit moet worden bepaald zowel bij de ontwikkeling van iColumbo en daarop aan te sluiten modules als bij elke verwerking in het kader van het eindgebruik. De verantwoordelijke is juridisch aanspreekbaar op de naleving van de Wbp. Indien anderen ingeschakeld worden voor de feitelijke verwerking van persoonsgegevens, moet de verantwoordelijk er zorg voor dragen dat ook deze partijen zich aan de Wbp houden.
5. Moet de verwerking van persoonsgegevens gemeld worden bij het College Bescherming Persoonsgegevens?
6. Wat is het doel van de verwerking? Voor elke afzonderlijke verwerking van persoonsgegevens moet gespecificeerd worden wat het legitieme doel is om de gegevens te mogen verwerken. Elk doel moet duidelijk, specifiek en in voldoende detail beschreven zijn.
7. Op welke van de in artikel 8 Wbp genoemde rechtmatige verwerkingsgronden kan de specifieke verwerking van persoonsgegevens worden gebaseerd? Is er sprake van toestemming van Internetgebruikers (c.q. werknemers bij de eindgebruiker), een contract, een wettelijke plicht of een legitiem belang dat zwaarder weegt dan het privacybelang van de betrokkenen?
8. Is er sprake van een verdere verwerking van gegevens? Zo ja, is (het doel van) de verdere verwerking verenigbaar is met het oorspronkelijk doel waarvoor gegevens verzameld zijn? Zo ja, dan is deze verdere verwerking toegestaan. Zo nee, dan is er sprake van een nieuwe verwerking en moet de vorige vraag (legitieme grondslag) opnieuw zelfstandig worden beantwoord.
9. Is er sprake van eerlijke, rechtmatige en veilige verwerking van persoonsgegevens?
   a. Zijn er maatregelen genomen om te garanderen dat gegevens correct, accuraat, adequaat, relevant en niet buiten proportioneel zijn met het oog op de doeleinden van verwerking?Worden niet meer data verwerkt dan noodzakelijk met het oog op het doel? Hier ligt een sterke samenhang met doelspecificatie (vraag 6).

[141] Indien het uitsluitend onder de politietaak valt, moeten de onderstaande vragen mutatis mutandis worden gelezen conform de Wet politiegegevens. Indien het uitsluitend onder de taak van inlichtingen- en veiligheidsdiensten valt, moeten de onderstaande vragen mutatis mutandis worden gelezen conform de afwijkende bepalingen van de Wiv 2002.

b. Worden gegevens niet langer (in identificeerbare vorm) bewaard dan noodzakelijk met het oog op het doel?
c. Worden gegevens voldoende beveiligd? Hierbij gaat het om zowel organisatorische als technische beveiligingsmiddelen die naar de stand van de techniek en kostenefficiënt een voldoende beveiligingsniveau garanderen.

10. Is er sprake van de verwerking van gevoelige gegevens (zoals gegevens betreffende ras, gezondheid, politieke overtuiging of seksuele voorkeur)? Wordt er beeldmateriaal verwerkt waarop personen identificeerbaar in beeld zijn (en waarop hun ras en eventuele gezondheid is af te lezen)? Zo ja, kan deze verwerking gegrond worden op een van de uitzonderingen genoemd in art. 17-23 van de Wbp? Zo nee, dan is de verwerking van gevoelige gegevens verboden.
11. Wordt voldaan aan de uit de Wbp voortvloeiende informatieplichten?
    a. Worden betrokken geïnformeerd over de gegevensverwerking?
    b. Worden betrokkenen in de gelegenheid gesteld hun inzage- en correctierechten uit te oefenen?
12. Worden persoonsgegevens doorgegeven aan derde landen (buiten de EU/EER)? Hebben die landen een passend beschermingsniveau? Zo nee, kan de verwerking op een van de uitzonderingsgronden in de Wbp gebaseerd worden (art. 75-77)?

Bijlagen

1. HDIeF, iRN en iColumbo

1.1. Aanleiding

Iedere handhavings- en opsporingsinstantie maakt gebruik van openbrononderzoek. Meestal ontwikkelen ze daarvoor een eigen systeem of koopt men een op de markt verkrijgbaar product in. Als gevolg hiervan heeft iedere onderzoeksinstantie eigen systemen, die specifiek voor de eigen onderzoeken en context ontwikkeld zijn. Gevolg hiervan is dat ieder systeem afgestemd is op het werk van deze specifieke dienst, maar ook dat veel werk dubbel gedaan wordt en dat de systemen van de verschillende diensten niet van elkaars mogelijkheden en valkuilen leren. iRN biedt de mogelijkheid om, aangevuld met de in ontwikkeling zijnde functionaliteiten van iColumbo, te dienen als een standaard-platform waar alle Nederlandse overheidsdiensten die zich met toezicht en handhaving bezighouden, gebruik van zouden kunnen maken.

1.2. iRN

Door de politie is het iRN (Internet Research & Investigation Network) ontwikkeld, waarbij opsporingsinstanties en overheidsdiensten met een toezichthoudende of controlerende wettelijke taak op een gecontroleerde manier het Internet kunnen gebruiken voor onderzoek, opsporing of surveillance. Dit houdt in dat de onderzoekers geen specifieke technische kennis behoeven te hebben om onderzoek te doen op het Internet, waarbij zaken als logging, opslag van gegevens en afscherming door het iRN-netwerk geregeld worden. Het iRN is hierbij in zekere zin te vergelijken met een Internet Service Provider (ISP) die geoptimaliseerd is voor handhavings- en opsporingsdiensten.

1.2.1. iRN als ISP

In de rol van ISP levert het iRN complete systemen met eigen Internetaansluiting aan de verschillende opsporingsinstanties. Deze systemen bevatten een Ubuntu Linux-installatie in twee varianten: een iRN Standaard-variant voor opsporing en onderzoek en een iRN Lite-variant, met een Windows-achtige uitstraling. Als gevolg hiervan kunnen opsporingsbeambten hier snel en adequaat mee overweg. De gebruikers van het systeem kunnen aan het begin van een sessie aangeven of zij herkenbaar (bijvoorbeeld als een met de politie geassocieerd IP-adres) of niet-herkenbaar het Internet op willen. De technische invulling van deze keuze wordt vervolgens door het systeem geregeld

Een andere belangrijke functionaliteit van het iRN (bij gebruik van iRN Standaard) is de logging-functionaliteit. Deze is toegevoegd aan het iRN, omdat de resultaten van het onderzoek van een eindgebruiker mogelijk zullen moeten dienen als bewijs in de rechtszaal. Om te kunnen dienen als bewijs, moet duidelijk zijn hoe dit bewijs verzameld is, en ook moet aangetoond worden dat er niet mee geknoeid is. Daarom wordt al het Internetverkeer gelogd dat door de gebruikers van iRN wordt gegenereerd, waarover een hash wordt berekend. Het berekenen van deze hash zorgt ervoor dat gecontroleerd kan worden of de data na opslag veranderd zijn.
De opgeslagen logs kunnen gebruikt worden in een rechtszaak, maar ook kan op basis hiervan de zogenaamde ‘iRN Replay’-functionaliteit worden ingevuld. Deze functionaliteit geeft een gebruiker de mogelijkheid om zijn eigen Internetgedrag terug te zien. De gebruiker kan een bepaalde Internetsessie opvragen, en vervolgens wordt de hele sessie opnieuw voor hem afgespeeld. Hierdoor kan een gebruiker precies terugkijken naar een onderzoek in het verleden, en achterhalen wat hij toen gezien heeft.

1.2.2. Open source

iRN is een volledig open source-gebaseerd netwerk. Dit houdt in dat alle broncode van iRN beschikbaar is voor autoriteiten om te onderzoeken of toetsen of de systemen correct functioneren. Dit is vereist om de resultaten van iRN te gebruiken als bewijsmateriaal, waarbij immers van belang is dat de resultaten op controleerbaar correcte wijze verkregen zijn en in de tussentijd ook niet aangepast zijn. Door open source-code te gebruiken en geen proprietary software, zal het altijd mogelijk zijn om de programmatuur te toetsen. Alle code in iRN moet dus

open source-gebaseerd zijn, in de zin dat deze beschikbaar is om door bevoegde instanties opgevraagd te worden.

1.2.3. iRN en open innovatie tussen de handhavings- en opsporingsdiensten

Op dit moment wordt iRN gebruikt binnen diverse handhavings- en opsporingsdiensten die voor de Nederlandse overheid werken. iRN is zo één netwerk dat door al deze instanties gebruikt wordt om onderzoek te doen. Hierdoor ontstaat een gezamenlijk platform waarop al deze onderzoekers kunnen samenwerken. Het voordeel hiervan is dat deze onderzoekers vanuit hun verschillende contexten oplossingen kunnen aandragen voor problemen, waardoor een bredere gebruikersgroep kan profiteren van deze oplossingen. Op dit moment is er een zogeheten *development cloud* ingericht, waar programmatuur kan worden ontwikkeld. Het idee hierachter is het stimuleren van innovaties door open ontwikkeling. Alle diensten die iRN/iColumbo gebruiken kunnen zo meewerken aan de ontwikkeling van deze hulpmiddelen. Verder wordt er communicatie tussen de ontwikkelaars voorzien door een forum, blog en een webruimte binnen de iRN-omgeving.

Op dit moment wordt iRN alleen door de Nederlandse overheid gebruikt. Wellicht wordt dit op termijn uitgebreid naar andere overheden. Door onder andere Europese opsporingspartners is al belangstelling getoond om het Nederlandse iRN/iColumbo-concept binnen Europa verder uit te bouwen. Ook op internationaal vlak zijn voordelen te behalen uit deze samenwerking. Het is wel nadrukkelijk de bedoeling dat iRN alleen aan overheidsinstanties ter beschikking wordt gesteld en niet aan private of commerciële partijen.

1.2.4. Verduurzaming iRN

iRN is gestart als een los project bij enkele politieregio's, maar is inmiddels zijn oorsprong ontgroeid. Inmiddels maken meer politieregio's gebruik van iRN, evenals andere handhavings- en opsporingsdiensten. Dit in combinatie met de hervorming van politieregio's maakt dat er gekeken moet worden hoe iRN opgehangen kan worden in de organisatie. Tijdens de interviews zijn er enkele mogelijkheden aan bod gekomen:

- iRN als geheel opnemen in een overheidsorganisatie, bijvoorbeeld het Ministerie van Binnenlandse Zaken. Hierbij kan de structuur verder gehandhaafd blijven en wordt iRN een overheidsorganisatie die diensten aan andere overheidsorganisaties levert. Dit maakt inzet binnen andere overheidsorganisaties eenvoudig, maar inzet binnen niet-Nederlandse organisaties minder eenvoudig.
- Een soort aandeelhoudersvergadering opzetten, waarbinnen alle gebruikers van iRN gezamenlijk verantwoordelijk zijn voor het onderhoud, doorontwikkelen en functioneren van iRN. Dit is een indeling waarbij iRN los komt te staan van de Nederlandse overheid, en mogelijk ook eenvoudiger kan samenwerken met andere overheden.

Op dit moment is nog niet duidelijk hoe iRN ingericht zal worden. Door de directies van NCTV, Belastingdienst, NFI en Nationale Politie is hiervoor in december 2011 het project Verduurzaming iRN/ontwikkeling iColumbo gestart met onder andere als opdracht een passend ondernemingsmodel voor een overheidsbreed iRN te realiseren.

1.3. iColumbo

Een volgende stap voor iRN is om naast de ISP-functionaliteit ook een openbrononderzoeks-functionaliteit aan te bieden. Dit houdt in dat het iRN niet alleen gecontroleerde toegang tot het Internet biedt, maar ook een analyse kan uitvoeren op de data verzameld van het Internet. Hiervoor is het iColumbo-project gestart. iColumbo is een onderdeel van iRN, dat als focus heeft om zelfstandig Internetonderzoek en analyse van de uit open Internetbronnen verzamelde data uit te voeren.

1.3.1. Doelstelling iColumbo

De doelstelling van iColumbo is om een open, controleerbaar platform te zijn dat gebruikt kan worden door verschillende opsporingsinstanties voor openbrononderzoek. iColumbo moet hierbij op basis van sleutelwoorden of andere informatie die door de eindgebruikers gedefinieerd wordt, zelfstandig informatie van het Internet verzamelen en analyseren om antwoord te geven op de oorspronkelijke zoekvragen van de eindgebruikers. Verder moet iColumbo ingepast worden

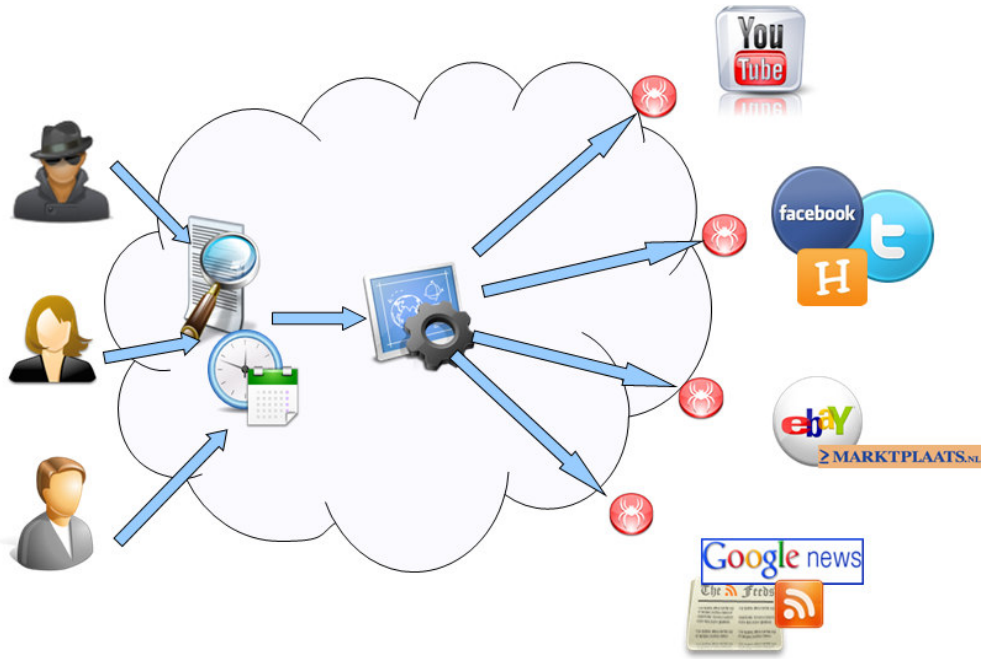
binnen iRN, wat betekent dat de garanties die iRN geeft wat betreft logging ook op iColumbo van toepassingen zijn.

1.3.2. Technische achtergrond iColumbo

iColumbo zal een centraal punt zijn voor de onderzoeken van de verschillende handhavings- en opsporingsdiensten. Alle zoekvragen die de gebruikers hebben worden in het systeem ingevoerd. Vervolgens zal het systeem een groot aantal Internetbronnen raadplegen. Belangrijke bronnen zijn:

- sociale media (bijvoorbeeld Twitter, Facebook);
- RSS-feeds van diverse websites (bijvoorbeeld nieuwsbronnen);
- online zoekmachines (bijvoorbeeld Google, Bing);
- eigen crawlers (dit zijn kleine zoekprogramma's die het Internet in kaart brengen, vergelijkbaar met de technologie die door de zoekmachines gebruikt worden).

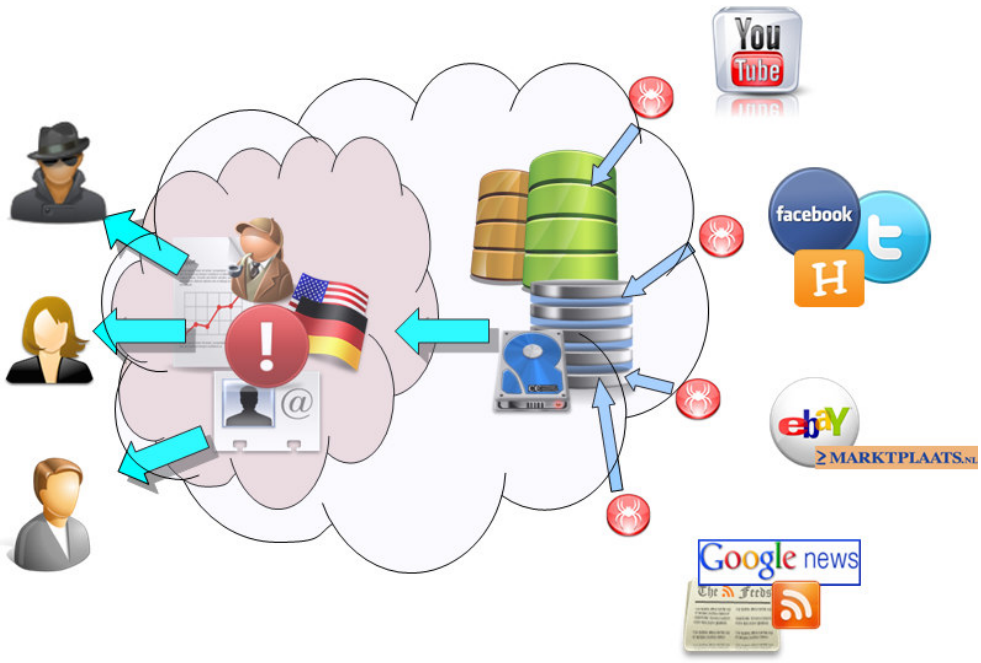
In onderstaand plaatje is het uitzetten van zoekopdrachten schematisch weergegeven. De witte wolk is het iRN/iColumbo-platform. De verschillende eindgebruikers (de personen links) verzenden hun zoekopdrachten naar iColumbo, dat na een verwerkingsslag de zoekopdracht uitzet bij de verschillende webpagina's.



Figuur 1: Het uitsturen van een zoekvraag door iColumbo

De resultaten van de zoekopdrachten worden door de webpagina's weer teruggestuurd naar iRN/iColumbo. Dit is weergegeven in **Error! Reference source not found.**2. Alle data wordt opgeslagen in de centrale server (om de informatie later als bewijs te kunnen gebruiken). Deze centrale server is een cluster van systemen dat in beheer is bij KPN. KPN zorgt er hierbij voor dat de data redundant opgeslagen worden, om voor een goede beschikbaarheid te zorgen. De eisen hiervoor worden door iRN geformuleerd.

Nadat de data opgeslagen zijn, maakt iColumbo (de donkere wolk) een analyseslag over de informatie. Doel van deze analyse is om de verschillende open bronnen te koppelen en vergelijken, resultaten te ontdubbelen, en zoekresultaten op een inzichtelijke manier te presenteren. Na deze analyse geeft iColumbo de eindgebruiker een antwoord dat aansluit op de zoekvraag. Hierbij kan ook onderscheid gemaakt worden al naar gelang de rechten die de verschillende gebruikers hebben.



Figuur 2. Het verzamelen en analyseren van de resultaten

1.3.3. iColumbo als platform

iColumbo is een platform waarin verschillende modules toegevoegd kunnen worden om de analyseresultaten van het systeem te verbeteren. Op dit moment wordt hierbij gebruik gemaakt van de Xtas-module, die meerdere soorten tekstuele analyses op data kan uitvoeren, en op basis waarvan verbanden tussen teksten kunnen worden gelegd en teksten onderling vergeleken kunnen worden. iColumbo kan aldus tekstuele analyses van open bronnen informatie uitvoeren en hierdoor sociale netwerken in kaart brengen.

Door de modulaire opzet van iColumbo is het mogelijk om later extra modules toe te voegen. Op dit moment ligt de focus op tekstanalyse, maar op termijn valt ook te denken aan socialenetwerkanalyse, video- en fotoherkenning en -analyse. Ook wordt gedacht aan het verwerken van technische gegevens die aan de data verbonden zijn (meta-data), denk bijvoorbeeld aan geografische data.

1.3.4. Juridische maatregelen in iColumbo

Met het oog de juridische aspecten van iColumbo is reeds een aantal maatregelen genomen. Ten eerste is alle informatie in iColumbo gekoppeld aan een dossier. Ieder dossier moet een doel hebben en een aangewezen aantal personen die hierbinnen aan het onderzoek werken. Op deze wijze wordt voorzien in doelbinding, aangezien alleen betrokken gebruikers toegang hebben tot de voor het onderzoek ingewonnen data. Iedere eindgebruiker kan (afhankelijk van zijn rechten) onderzoeken starten en bepaalde functionaliteit inzetten. Verder moet bij ieder dossier worden vastgelegd welke functionaliteit gebruikt mag worden binnen dit dossier en op grond van welke grondslag dit onderzoek geschiedt. Er kan hierbij ook voor gekozen worden om een verwijzing op te nemen naar een expliciete toestemming van een bevoegde autoriteit voor de inzet van bepaalde functionaliteiten. Het systeem zal deze verwijzing niet kunnen controleren, maar het systeem ondersteunt hiermee wel de controleerbaarheid achteraf. Tevens wordt, zoals al gezegd, alle activiteit van het systeem gelogd voor bewijsdoeleinden.

1.4. HDIeF

Herkenning Digitale Informatie en Fingerprinting (HDIeF) is een programma van de NCTV, dat eind 2009 gestart is en loopt tot medio 2012. Hierin wordt onderzoek gedaan naar het inzetten van technieken voor het geautomatiseerd herkennen van digitale gegevens. Dit kan zijn in tekst, beeld, en geluid. Doelstelling hiervan is om de ontwikkelde technologie ten goede te laten komen voor handhavings- en opsporingsorganisaties. Door het gebruik van geautomatiseerde

herkenningstechnologie zullen organisaties beter in staat zijn hun handhavende of opsporingstaken uit te oefenen.

Op dit moment richt het programma zich vooral op de volgende aspecten:

- herkennen van personen (gedragsherkenning, identiteit vaststellen);
- herkennen van objecten;
- herkennen van teksten;
- herkennen van (delen van) bestanden (audio, video, foto);
- herkennen van gebruikte opnameapparatuur;
- herkennen van verborgen boodschappen en sociale netwerkstructuren.

Binnen het programma zijn enkele projecten gestart die zich bezighouden met de ontwikkeling van technieken als het zoeken in videobestanden en het herkennen van tekst in grafische bestanden. De belangrijkste functionaliteiten die momenteel binnen iColumbo tot stand worden gebracht zijn persoonsherkenning en het leggen van verbanden tussen verschillende stukken tekst.

Het HDIeF-programma zal enkele technologieën en hulpmiddelen opleveren die goed ingepast kunnen worden binnen het iColumbo-platform. Hoe de integratie precies uitgevoerd zal gaan worden is nog niet duidelijk, maar de resultaten van het HDIeF-programma zullen naar verwachting toegevoegde waarde hebben voor het systeem. De doelstelling van HDIeF is om technologie te ontwikkelen die beschikbaar komt voor Nederlandse opsporingsinstanties. Omdat iColumbo modulair is opgezet en via iRN beschikbaar is voor een breed scala aan Nederlandse overheidsdiensten, is iColumbo zeer geschikt om resultaten uit het HDIeF-programma in te integreren. Zo kunnen bijvoorbeeld ontwikkelde functionaliteiten voor een verbeterde selectie en presentatie van gegevens worden ingepast in iColumbo.

2. Onderzoeksbronnen

2.1. Geïnterviewde personen

Opdrachtgever

But Klaasen	NCTV

Eindgebruikers

Eric Hertogh	Belastingdienst
Toon Steenbakkers	Douane
Pieter van Lierop	FIOD-ECD
Rein Tellier	Politie Alkmaar
Edwin Posthumus	Politie Groningen

Ontwikkelaars

Peter de Beijer	iRN
Ork de Rooij	Universiteit van Amsterdam
Corné Versloot	TNO

2.2. Deelnemers workshop eindgebruikers

Robert Augusteijn	iColumbo
Christiaan Baardman	Gerechtshof Den Haag, kenniscentrum Cybercrime
Peter de Beijer	politie Gelderland-Zuid, iRN
Monique Boddaert	NCTV
Maarten Bras	DNB
Tim Cooijmans	Radboud Universiteit Nijmegen
Eric Hertogh	Belastingdienst
Bart Jonkers	NCTV
Pieter van Lierop	FIOD-ECD
Edwin Posthumus	politie Groningen
Toon Steenakkers	Douane
Ronny Wichers Schreur	Radboud Universiteit Nijmegen
Ivo Vis	AFM

3. Samenstelling begeleidingscommissie

P. Albers	Ministerie van Veiligheid en Justitie
C.A. Baardman	Gerechtshof 's-Gravenhage
F. Bacco	Ministerie van Defensie
P. de Beijer	politie Gelderland-Zuid, iRN
A.M.A. Hertogh	Belastingdienst
M. Israel	Nederlands Forensisch Instituut
E.C. Mac Gillavry	Wetenschappelijk Bureau Openbaar Ministerie
L.P. Mol Lous	Ministerie van Veiligheid en Justitie

4. Literatuurlijst

Ardagna, Claudio A. e.a., 'Privacy Models and Languages: Access Control Policies', in: J. Camenisch, R.E. Leenes, D. Sommer (eds), *Privacy and Identity Management for Europe (PRIME)*, Heidelberg etc: Springer, 2007.

Attema, J. en D. de Nood (2010), *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit*, WRR web-publicatie nr. 47.

Buruma, Y. & L.J. Verborg (2008), 'Artikel 126j', in: Melai/Groenhuijsen e.a., *Wetboek van Strafvordering*, Kluwer.

Buruma, Y. (2001) *Buitengewone opsporingsmethoden*. Deventer: Tjeenk W.E.J. Willink.

Cavoukian, A. (2010), 'Privacy by design: the definitive workshop', *Identity in the Information Society* 3(2), p. 247-251.

Davet, G. (2008), 'Edvige: le projet de décret de Michèle Allot-Marie', *Le Monde*, 18 september 2008, http://www.lemonde.fr/societe/article/2008/09/18/edvige-le-projet-de-decret-de-michele-alliot-marie_1096633_3224.html.

De Hert, P. en S. Gutwirth (2009), 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action', in S. Gutwirth e.a. (red.), *Reinventing Data Protection?*. Berlin: Springer, p. 57-71.

Gallup (2008), *Data Protection in the European Union*, Flash Eurobarometer Series #225.

Koffijberg, J., S. Dekkers, G. Homburg B. van den Berg (2009), *Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Regioplan publicatienr. 1774.

Koops, B.J. et al. (2012), *D3.4 Code as Code Assessment*, VIRTUOSO deliverable, April 2012, http://www.virtuoso.eu/VIRTUOSO/servlet/document.fileView/D3.4%20Code%20as%20code%20assessment_v1.0_Apr2012def.pdf.

Kranzberg, M. (1986), 'Technology and History: "Kranzberg's Laws"', *Technology and Culture* 27(3), p. 544-560.

Laufer, R.S. & Wolfe, M. (1977), 'Privacy as a concept and a social issue: A multidimensional developmental theory', *Journal of Social Issues* 33(3), p. 22-42.

Leenes, R.E. (2010), *Harde lessen. Apologie van technologie als reguleringsinstrument*, oratie UvT, Tilburg.

Lessig, L. (1999), *Code and other laws of cyberspace*, New York, NY: Basic Books.

Marc van Lieshout, Linda Kool, Gabriela Bodea, Bas van Schoonhoven, James Schlechter (2012), *Stimulerende en remmende factoren voor Privacy by Design in Nederland*, Delft: TNO-rapport.

Ohm, P. (2010), 'Broken Promises of Privacy. Responding to the Surprising Failure of Anonymization', *UCLA Law Review* 57, p. 1701-1777.

Reinsma, M. en H. van der Sluijs (2002), *Naar ruimere openbaarheid en een vrij gebruik van bestuurlijke informatie*, rapport in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, december 2002.

SCP (Sociaal Cultureel Planbureau) (2011), *De sociale staat van Nederland 2011*, SCP: Den Haag, http://www.scp.nl/Publicaties/Alle_publicaties/Publicaties_2011/De_sociale_staat_van_Nederland_2011.

Steffek, J. (2003), 'The legitimation of international governance: A discourse approach', *European Journal of International Relations* 9 (2), p. 249-275.

TAPAC (2004), *Safeguarding privacy in the fight against terrorism*, Report for the Technology and Privacy Advisory Committee, 1 maart 2004, http://www.defense.gov/news/Jan2006/d20060208tapac.pdf.

Technology Review (2006), *The total information awareness project lives on*, door M. Williams, 26 april 2006, http://www.technologyreview.com/Infotech/16741/?a=f.

TNS-NIPO (2011), *Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer 359.

Van der Meulen, N. & B.J. Koops (2011), 'The Challenge of Identity Theft in Multi-Level Governance. Towards a Coordinated Action Plan for Protecting and Empowering Victims', in:

R. Letschert & J. van Dijk (eds), *The New Faces of Victimhood*, Dordrecht etc.: Springer, p. 159-190.
Vedder, A. (2008), 'Responsibilities for Information on the Internet', in: K. Himma and H. Tavani (eds.), *The Handbook of Information and Computer Ethics,* Hoboken, NJ (etc.): John Wiley and Sons, p. 339-359.
Vedder, A. (2011), 'Legitimiteit, verantwoordelijkheid, vertrouwen en acceptatie', in: L. Kool e.a. (2011) *Trusted Technology: Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de elektronische dienstverlening van de overheid.* TNO en TILT.
Walden, Ian (2007), *Computer Crimes and Digital Investigations*, Oxford: Oxford UP.
Weyers, H. en M. Hertogh (2007), *Legitimiteit betwist. Een verkennend literatuuronderzoek naar de ervaren legitimiteit van het justitieoptreden,* Groningen, WODC-rapport, http://wodc.nl/onderzoeksdatabase/legitimiteit-van-recht-en-rechtspraak.aspx.
WRR (Wetenschappelijke Raad voor het Regeringsbeleid) (2011), *iOverheid*, Den Haag: WRR.
Zwenne, G.-J. & L. Mommers (2010), 'Zijn foto's en beeldopnamen 'rasgegevens' in de zin van artikel 126nd Sv en artikel 18 Wbp?', *Privacy & informatie* nr. 5, p. 237-247.